COLLECTION QUEYSANNE-REVUZ

MATHEMATIQUE

Tome 1

NOMBRES
PROBABILITES

TERMINALES
C E

FERNAND NATHAN

NOUVELLE COLLECTION DIRIGÉE

PAR

MICHEL QUEYSANNE
Ancien élève de l'E.N.S.
Maître assistant à l'Université
de Paris VII

ANDRÉ REVUZ
Ancien élève de l'E.N.S.
Professeur à l'Université
de PARIS VII

MATHÉMATIQUE

par
MICHELE DEBRAY
Ancienne élève de l'E.N.S. Sèvres
Professeur agrégé au Lycée Albert Camus

DANIEL REVUZ
Ancien élève de l'Ecole Polytechnique
Docteur ès Sciences

et
MICHEL QUEYSANNE

TERMINALE CE

tome 1

NOMBRES • PROBABILITÉS

FERNAND NATHAN EDITEUR
18, rue Monsieur-le-Prince, PARIS VI

A la même Librairie

COLLECTION QUEYSANNE-REVUZ

SECOND CYCLE

- **MATHÉMATIQUE** classes de 2e A et 2e A B *(Programme 73)*
- **MATHÉMATIQUE** classes de 2e C T *(Programme 73)*
- **MATHÉMATIQUE** classe de 1re A B
  Tome 1
  Tome 2
- **MATHÉMATIQUE** classes de 1re C D E
  Tome 1
  Tome 2
- **MATHÉMATIQUE** classe terminale A
- **MATHÉMATIQUE** classe terminale B
- **MATHÉMATIQUE** classes terminales C D E
  Tome 1 : Terminale C E Nombres - Probabilités
  Tome 1 : Terminale D Nombres - Probabilités - Géométrie
  Tome 2 : Terminale C D E Analyse
  Tome 3 : Terminale C E Géométrie

EXERCICES ET PROBLÈMES RÉSOLUS DE MATHÉMATIQUE

- Classes de 2e A et 2e A B
- Classe de 2e C T
- Classe de 1re C D E
- Classe de Terminale C E
  Tome 1
  Tome 2
- Classes de Terminale D

© *Éditions Fernand Nathan 1974*

Toute reproduction, même partielle, de cet ouvrage est interdite. Une copie ou reproduction par quelque procédé que ce soit, photographie, photocopie, microfilm, bande magnétique, disque ou autre, constitue une contrefaçon passible des peines prévues par la loi du 11 mars 1957 sur la protection des droits d'auteur.

Avant-propos

Les programmes des Terminales C et E étant très voisins, notre collection présente pour ces classes un cours commun réparti en trois tomes :

Tome *I*. Nombres *et* probabilités *(Sections I, II et VIII des programmes).*
Tome *II*. Analyse *(Sections III, IV et V des programmes).*
Tome *III*. Géométrie *(Section VI et VII des programmes).*

Les parties, très peu nombreuses, qui n'appartiennent qu'à l'un des programmes des classes C ou E sont clairement indiquées.

✳

Comme il a été dit plus haut, ce tome I est consacré à l'étude des ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$ *et* $\mathbb{C}$ *et à celle des probabilités sur un ensemble fini.*

Dans les chapitres 1, 2 et 3, consacrés respectivement aux entiers naturels, *aux* entiers relatifs *et aux* nombres réels, *nous avons, conformément au préambule des programmes, présenté, tout au long de l'exposé, des révisions et quelques compléments relatifs aux notions fondamentales d'algèbre. Pour pouvoir exposer convenablement la représentation décimale des nombres réels, nous avons traité dans le chapitre 3 l'étude des suites de nombres réels bien que cette étude figure dans la section V du programme (Exemples de fonctions d'une variable réelle).*

Le chapitre 4 est consacré aux nombres complexes. *Nous avons fait précéder l'exposé d'un rappel des principales propriétés des* espaces vectoriels sur $\mathbb{R}$. *De même l'étude de la représentation géométrique d'un nombre complexe par un vecteur de l'*espace vectoriel euclidien $\mathcal{E}_2$ *ou par un point de l'*espace affine euclidien E_2 *est accompagnée d'une révision des résultats essentiels concernant ces deux espaces. Enfin la représentation trigonométrique des nombres complexes est l'occasion d'une révision systématique des formules de* trigonométrie.

Le chapitre 5 traite des probabilités; il est la suite naturelle de l'étude concrète des phénomènes aléatoires effectuée en classe de Première.

Nous avons complété ces cinq chapitres par trois annexes.
L'annexe A regroupe les propriétés fondamentales des lois de composition interne *qui ont été revues, conformément au préambule des programmes, chaque fois que l'occasion s'en présentait dans les chapitres 1, 2 et 3. Nous pensons que cette deuxième présentation de ces définitions, cette fois dans un ordre systématique, rendra service au lecteur.*

L'annexe B présente une introduction à la théorie des cardinaux, *en particulier des cardinaux finis, c'est-à-dire des* entiers naturels. *Nous espérons que, bien que ne figurant pas au programme, ces notions intéresseront certains lecteurs.*

L'annexe C est consacrée à la construction du groupe $(\mathbb{Z}, +)$. *Cette étude n'appartient certainement pas au programme de terminale E. Quant aux élèves de terminale C, la construction de* $\mathbb{Z}$ *nécessitant l'emploi d'une loi-quotient assez compliquée, nous pensons que l'étude des notions constituant cette annexe sera plus fructueuse après l'étude des sections I et II du chapitre 2, en particulier lorsque auront été étudiées les lois-quotients définissant les opérations dans* $\mathbb{Z}/n\mathbb{Z}$.

Ce tome I se termine, enfin, par un index terminologique comprenant tous les termes importants utilisés dans ce volume.

M. Q. et A. R.

PROGRAMME DE TERMINALE C

Arrêté du 14 mai 1971
B.O.E.N. 25 (24-6-71)

Préambule

a) Les paragraphes marqués d'un astérisque ne peuvent faire l'objet de questions de cours, écrites ou orales, ni être utilisés, en mathématiques, à l'occasion d'un problème ou d'un exercice d'application à l'écrit ou à l'oral du baccalauréat.

b) Les rubriques du programme comportent un ordre d'énumération. Cet ordre exprime parfois une intention dont les professeurs pourront s'inspirer, mais il ne saurait être imposé; par exemple il est loisible de permuter les trois alinéas du I.3 concernant les nombres entiers, les III.1 et 2 (notions de continuité et de limite), de donner, en II.3, une autre introduction des nombres complexes, etc.

c) Chaque fois que l'occasion s'en présentera on mettra en évidence, sur les exemples étudiés dans les différents chapitres, les structures de groupe, sous-groupe, anneau, corps, espace vectoriel, ainsi que les isomorphismes et homomorphismes (noyau), automorphismes rencontrés.

I. Nombres entiers naturels — Arithmétique

1. Énoncé des propriétés attribuées à l'ensemble $\mathbb{N}$ des entiers naturels. Raisonnement par récurrence. Applications de $\mathbb{N}$ dans un ensemble X; notation indicielle; exemples.

2. Anneau $\mathbb{Z}$ des entiers relatifs; multiples d'un entier relatif : notation $n\mathbb{Z}$. Congruences modulo n; l'anneau $\mathbb{Z}/n\mathbb{Z}$; division euclidienne dans $\mathbb{Z}$, dans $\mathbb{N}$. Principe des systèmes de numération; base; numérations décimale et binaire.

3. *a)* Nombres premiers dans $\mathbb{Z}$; si p est premier, $\mathbb{Z}/p\mathbb{Z}$ est un corps.

b) Décomposition d'un entier naturel en facteurs premiers; existence, unicité.

c) Plus grand commun diviseur et plus petit commun multiple; nombres premiers entre eux; identité de Bezout.
(L'ordre de *a*), *b*), *c*) est, bien entendu, laissé au choix du professeur.)

II. Nombres réels; calcul numérique; nombres complexes

1. Inventaire (sans démonstration) des propriétés de $\mathbb{R}$: c'est un corps commutatif totalement ordonné (révision); toute partie non vide majorée admet un plus petit majorant; tout intervalle de $\mathbb{R}$ contenant plus d'un point contient un nombre rationnel.

2. Valeurs décimales approchées à 10^{-n} près, par défaut et par excès, d'un nombre réel.
Représentation d'un nombre réel par une suite décimale illimitée (l'étude de la périodicité n'est pas au programme).
Valeurs approchées d'un nombre réel, encadrement, incertitude absolue et relative.
Valeurs approchées d'une somme, d'une différence, d'un produit, d'un quotient de nombres réels dont on connaît des valeurs approchées. De nombreux exercices de calcul numérique seront faits à l'occasion de l'étude des fonctions usuelles et à l'occasion de problèmes, pour mettre en application les notions de valeurs approchées, d'encadrement, d'ordre de grandeur d'un résultat, d'incertitude (cf. V.8).

3. L'addition et la multiplication des matrices 2×2 munissent l'ensemble $\mathbb{C}$ des matrices à coefficients réels de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ d'une structure de corps commutatif. Identification de $\mathbb{R}$ à un sous-corps de $\mathbb{C}$ par l'application $a \longmapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$; $\mathbb{C}$ est un espace vectoriel de dimension deux sur $\mathbb{R}$. Notation $a + bi$; nombre complexe; nombres complexes conjugués; module d'un nombre complexe.

4. Homomorphisme θ de $\mathbb{R}$ sur le groupe multiplicatif des nombres complexes de module 1 (rappel de Première); forme trigonométrique d'un nombre complexe non nul : $r(\cos x + i \sin x)$ avec $r > 0$ et $x \in \mathbb{R}$; argument d'un tel nombre (classe des nombres x ou, par abus de langage, l'un d'eux).

Calcul de cos nx et de sin nx ($x \in \mathbb{R}$, $n = 2, 3, 4$) et linéarisation des polynômes trigonométriques. Existence et représentation géométrique des racines n-ièmes d'un nombre complexe.

5. Résolution des équations du premier et du second degré à coefficients complexes; calcul des parties réelles et imaginaires des racines; cas des coefficients réels.

III. Calcul différentiel

1. *Fonctions numériques d'une variable réelle : continuité*

Continuité « en un point »; continuité sur un intervalle; somme, produit, quotient de fonctions continues; continuité de la fonction composée de deux fonctions continues (sans démonstration).
On admettra sans démonstration le théorème suivant : « si une fonction est continue sur un intervalle, l'image, par la fonction, de cet intervalle est un intervalle ». Application à une fonction continue et strictement monotone sur un intervalle : existence de la fonction réciproque; monotonie et continuité de cette fonction (on admettra la continuité).

2. *Fonctions numériques d'une variable réelle : limites*

Limite d'une fonction lorsque la variable tend vers un nombre réel donné, vers l'infini. Unicité. Cas particulier des suites.
Limite d'une somme, d'un produit, d'un quotient (sans démonstration).

3. *Fonctions numériques d'une variable réelle : dérivation*

Révision du programme de Première C : fonction linéaire tangente en un point à une fonction donnée; notation différentielle; dérivée en ce point. Fonction dérivée; dérivée d'une somme, d'un produit, d'un quotient de fonctions dérivables. Interprétation géométrique de la dérivée (repère cartésien); équation de la tangente. Définition des dérivées successives.
Dérivée en un point de la composée de deux fonctions dérivables. Dérivée en un point de la réciproque d'une fonction dérivable et strictement monotone.
On admettra sans démonstration que si une fonction numérique est dérivable sur un intervalle et si sa dérivée est positive ou nulle, elle est croissante au sens large sur cet intervalle.
Comparaison de deux fonctions ayant même fonction dérivée sur un intervalle.
Étude du sens de variation d'une fonction dérivable à l'aide du signe de sa dérivée. Représentation graphique; exercices simples de recherche d'asymptotes.

4. *Fonctions vectorielles d'une variable réelle*

Application d'une partie de $\mathbb{R}$ dans un espace vectoriel euclidien de dimension finie.
Continuité en un point; limite d'une fonction lorsque la variable tend vers un nombre réel donné, vers l'infini.
Dérivée en un point; si l'espace vectoriel est rapporté à une base, coordonnées, dans cette base, de la dérivée; fonction dérivée.
Dérivée d'une somme de fonctions vectorielles dérivables, du produit d'une fonction vectorielle dérivable par une fonction numérique dérivable.
Dérivée du produit scalaire de deux fonctions vectorielles dérivables. Application à la recherche de tangentes; exemples des coniques et des hélices circulaires.

5. *Cinématique du point*

Mouvement d'un point : application d'un intervalle de $\mathbb{R}$ dans un espace affine euclidien. Trajectoire.
Vecteur-vitesse à un instant donné. Un repère étant choisi, coordonnées du vecteur-vitesse dans ce repère. Norme du vecteur-vitesse.
Vecteur-accélération à un instant donné. Un repère étant choisi, coordonnées du vecteur-accélération dans ce repère.
Étude des mouvements circulaires (vitesse angulaire); étude des mouvements hélicoïdaux uniformes.

IV. Calcul intégral

1. Définition des sommes de Riemann d'une fonction numérique d'une variable réelle sur un intervalle fermé, borné. Existence de l'intégrale pour une fonction monotone; notation $\int_a^b f(t)\,dt$; premières propriétés. On admettra que ces propriétés s'étendent à des fonctions continues, ou monotones par morceaux.
Moyenne d'une telle fonction sur un intervalle fermé, borné. Lien avec la dérivation en des points où la fonction est continue.

Primitives; ensemble des primitives; égalité $\int_a^b f(t)\,dt = F(b) - F(a)$, f étant continue sur $[a, b]$ et admettant F pour primitive.
Calcul de primitives; intégrales par parties.

2. On énoncera, sans démonstration, les propriétés des aires dont l'existence est admise ici (additivité, unité d'aire...)
Application du calcul intégral à l'évaluation de l'aire de la partie de $\mathbb{R} \times \mathbb{R}$ définie par $a \leqslant x \leqslant b$ $0 \leqslant y \leqslant f(x)$; f étant une fonction positive monotone par morceaux, puis une fonction positive continue.
Extensions à $b < a$ et à une fonction négative.

3. *Applications géométriques, mécaniques, physiques etc. (calcul de volumes, masses, moments d'inertie; vitesse et distance parcourue; intensité et quantité d'électricité; puissance et énergie, etc.).
Valeur efficace d'un phénomène périodique.
(Le paragraphe IV.3 ne fait pas partie — voir Préambule a) — du programme des épreuves de mathématiques du baccalauréat.)

V. Exemples de fonctions d'une variable réelle

Certains résultats de ce chapitre, déjà connus des élèves, pourront illustrer les chapitres précédents; il sera opportun de répartir les différentes rubriques de celui-ci entre plusieurs moments de l'année.

1. *Fonction* $x \longmapsto x^n$ $(n \in \mathbb{Z})$; dérivée; primitives.

2. *Fonction* $x \longmapsto x$ $(r \in \mathbb{Q}, x > 0)$; dérivée; primitives.

3. *Suites* arithmétiques et géométriques. Somme des n premiers termes.

4. *Fonctions circulaires*; dérivées (révision); dérivées et primitives de $x \longmapsto \cos(ax + b)$ et $x \longmapsto \sin(ax + b)$.

5. *Logarithme népérien* (notation Log) : $\operatorname{Log} x = \int_1^x \frac{dt}{t}$ $(x > 0)$.

Limite, quand la variable positive x tend vers l'infini, de Log x et de $\frac{\operatorname{Log} x}{x}$. Limite, quand x tend vers 0, de x Log x. Représentation graphique.

6. *Fonction exponentielle* (notation exp).

Propriétés; dérivée; représentation graphique; nombre e; notation e^x; limite de $\frac{e^x}{x}$ quand x tend vers $+\infty$.

7. *Autres fonctions logarithmiques et exponentielles*

Relations entre les fonctions exponentielle et logarithmique de base a, et celles de base e.
Définition de x^α où $\alpha \in \mathbb{R}$; dérivée de la fonction $x \longmapsto x^\alpha$.
*Notation e^{ix} pour désigner $\cos x + i \sin x$; ω étant une constante réelle, dérivée de la fonction $x \longmapsto e^{i\omega x}$.

Remarque : l'étude d'exemples de fonctions composées du type logarithmique ou exponentiel sera strictement limitée aux cas où sont en évidence les intervalles sur lesquels la dérivée garde un signe constant et où les indéterminations à lever sont uniquement celles qui ont été énumérées plus haut.

8. *Calcul numérique*

Usage de la règle à calcul.
Usage de tables; pratique de l'interpolation linéaire; tables de logarithmes.
Usage de machines à calculer de bureau.

9. **Équations différentielles*

Recherche des fonctions numériques une ou deux fois dérivables de la variable réelle x vérifiant les équations :
$y' = ay$, a étant une constante réelle,
$y'' + \omega^2 y = 0$, ω étant une constante réelle non nulle (on admettra que les solutions forment un espace vectoriel de dimension 2).
(Le paragraphe V.9 — voir Préambule a) — ne fait pas partie du programme des épreuves de mathématiques du baccalauréat.)

VI. Éléments de géométrie affine et euclidienne

N. B. : Dans ce paragraphe le corps de base est $\mathbb{R}$ et la dimension n est toujours égale à 2 ou 3. Une « transformation d'un ensemble E » est une bijection de E sur lui-même ; une application f de E dans lui-même est une involution si $f \circ f$ est l'identité : c'est une transformation de E.

1. Somme directe de deux sous-espaces vectoriels ; sous-espaces vectoriels supplémentaires. Application linéaire d'un espace vectoriel E dans un espace vectoriel F : image et noyau. Addition et composition des applications linéaires.
Groupe linéaire. Homothéties vectorielles.

2. Barycentre dans un espace affine. Variété affine. Repère affine. Réduction, dans le cas euclidien, de $f(M) = a\,MA^2 + b\,MB^2 + c\,MC^2$.

3. Application affine d'un espace affine E dans lui-même, application linéaire associée.
Exemples : projection parallèle sur un sous-espace affine ; involutions affines, leurs points fixes ; translations et homothéties.

4. Applications linéaires d'un espace vectoriel euclidien dans lui-même conservant la norme ; transformations orthogonales (isométries vectorielles), groupe orthogonal.
Dans le plan vectoriel et dans l'espace vectoriel de dimension trois, éléments fixes des transformations orthogonales involutives (symétries). Orientation du plan vectoriel euclidien (rappel de la classe de Première).
Étude des rotations vectorielles de l'espace vectoriel euclidien de dimension trois (par définition, une telle rotation est, soit l'identité, soit une transformation orthogonale qui a pour seuls éléments fixes ceux d'une droite vectorielle) ; groupe des rotations vectorielles ; orientation de l'espace.
Produit vectoriel, dans l'espace vectoriel euclidien orienté de dimension trois.

5. Définition d'une isométrie de l'espace affine euclidien. Toute isométrie est une bijection affine. Groupe des isométries ; sous-groupe des déplacements.
Dans le plan affine euclidien, symétries, translations, rotations : tout déplacement est de l'un de ces deux derniers types.
Dans l'espace affine euclidien de dimension trois, symétries, translations, rotations, vissages ; tout déplacement est de l'un de ces trois derniers types.
Exemples simples de groupes d'isométries laissant invariant un ensemble donné.

VII. Compléments de géométrie euclidienne plane

1. Angle d'un couple de demi-droites vectorielles (rappel de Première) ; groupe $\mathcal{A}$ des angles de demi-droites.
Angle d'un couple de droites vectorielles (ensemble des deux rotations vectorielles transformant la première en la seconde) ; groupe $\mathcal{A}'$ des angles de droites. Homomorphisme canonique $\mathcal{A} \longrightarrow \mathcal{A}'$; son noyau. Isomorphisme $\mathcal{A}' \longrightarrow \mathcal{A}$ déduit de l'homomorphisme $\alpha \longrightarrow \alpha + \alpha$ de $\mathcal{A}$ sur $\mathcal{A}$. Condition, en termes d'angles de droites, pour que quatre points soient cocycliques.

2. Similitudes planes (c'est-à-dire applications du plan dans lui-même conservant les rapports de distances). Représentation par les formules $z' = az + b$ ou $z' = \bar{a}z + b$ lorsque l'on a identifié le plan à $\mathbb{C}$ grâce au choix d'un repère orthonormé. Points fixes des similitudes. Groupe des similitudes du plan et sous-groupes remarquables.

3. Étude des courbes représentées, dans un repère orthonormé, par des équations de la forme $ax^2 + by^2 + 2cx + 2dy + e = 0$ ($|a| + |b| \neq 0$). Différentes formes de ces courbes ; existence d'axes ou de centres de symétrie, d'asymptotes ; équations réduites ; existence de la tangente. Ellipse, hyperbole, parabole définies par les propriétés de leurs points qui font intervenir les foyers et directrices (les propriétés des tangentes aux coniques sont hors du programme).
Équation de l'hyperbole rapportée à ses asymptotes.

VIII. Probabilités sur un ensemble fini

1. Espaces probabilisés finis $(\Omega, \mathcal{B}(\Omega), p)$.
Applications mesurables (ou variables aléatoires) ; probabilité image, fonction de répartition d'une variable aléatoire réelle.
Couple de variables aléatoires réelles, loi du couple. Lois marginales. Couple indépendant. Système de n variables aléatoires indépendantes.

2. Espérance mathématique d'une variable aléatoire à valeurs dans $\mathbb{R}$ ou $\mathbb{R}^2$.
Espérance mathématique de la somme des deux variables aléatoires réelles d'un couple, du produit dans le cas d'un couple indépendant.
Variance, écart-type d'une variable aléatoire réelle.

3. Inégalité de Bienaymé-Tchebycheff. Épreuves répétées ; loi faible des grands nombres.

PROGRAMME DE TERMINALE E

Arrêté du 14 mai 1971
B.O.E.N. 25 (24-6-71)

Préambule

a) Les paragraphes marqués d'un astérisque ne peuvent faire l'objet de questions de cours, écrites ou orales, ni être utilisés, en mathématiques, à l'occasion d'un problème ou d'un exercice d'application à l'écrit ou à l'oral du baccalauréat.

b) Les rubriques du programme comportent un ordre d'énumération. Cet ordre exprime parfois une intention dont les professeurs pourront s'inspirer, mais il ne saurait être imposé; par exemple il est loisible de donner, en II. 3 une autre introduction des nombres complexes, de permuter les III.1 et 2 (notions de continuité et de limite) etc.

c) Chaque fois que l'occasion s'en présentera on mettra en évidence, sur les exemples étudiés dans les différents chapitres, les structures de groupe, sous-groupe, anneau, corps, espace vectoriel, ainsi que les isomorphismes et homomorphismes (noyau), automorphismes rencontrés.

I. Nombres entiers naturels — Arithmétique

Exemples de raisonnement par récurrence.
Exemples d'emploi de la notation indicielle.
Principe des systèmes de numération; base; numérations décimale et binaire.

II. Nombres réels; calcul numérique; nombres complexes

1. Inventaire (sans démonstration) des propriétés de $\mathbb{R}$: c'est un corps commutatif totalement ordonné (révision); toute partie non vide majorée admet un plus petit majorant; tout intervalle de $\mathbb{R}$ contenant plus d'un point contient un nombre rationnel.

2. Valeurs décimales approchées à 10^{-n} près, par défaut et par excès, d'un nombre réel.
Représentation d'un nombre réel par une suite décimale illimitée (l'étude de la périodicité n'est pas au programme).
Valeurs approchées d'un nombre réel, encadrement, incertitudes absolue et relative.
Valeurs approchées d'une somme, d'une différence, d'un produit, d'un quotient de nombres réels dont on connaît des valeurs approchées.
De nombreux exercices de calcul numérique seront faits à l'occasion de l'étude des fonctions usuelles et à l'occasion de problèmes, pour mettre en application les notions de valeurs approchées, d'encadrement, d'ordre de grandeur d'un résultat, d'incertitude (cf. V.8).

3. L'addition et la multiplication des matrices 2×2 munissent l'ensemble $\mathbb{C}$ des matrices à coefficients réels de la forme $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ d'une structure de corps commutatif. Identification de $\mathbb{R}$ à un sous-corps de $\mathbb{C}$ par l'application $a \longmapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$; C est un espace vectoriel de dimension deux sur $\mathbb{R}$. Notation $a + bi$; nombre complexe; nombres complexes conjugués; module d'un nombre complexe.

4. Homomorphisme θ de $\mathbb{R}$ sur le groupe multiplicatif des nombres complexes de module 1 (rappel de Première); forme trigonométrique d'un nombre complexe non nul : $r(\cos x + i \sin x)$ avec $r > 0$ et $x \in \mathbb{R}$; argument d'un tel nombre (classe des nombres x ou, par abus de langage, l'un d'eux). Calcul de $\cos nx$ et de $\sin nx$ ($x \in \mathbb{R}$, $n = 2, 3, 4$), et linéarisation des polynômes trigonométriques.
Existence et représentation géométrique des racines n-ièmes d'un nombre complexe.

5. Résolution des équations du premier et du second degré à coefficients complexes; calcul des parties réelles et imaginaires des racines; cas des coefficients réels.

III. Calcul différentiel

1. *Fonctions numériques d'une variable réelle : continuité*
Continuité « en un point »; continuité sur un intervalle; somme produit, quotient de fonctions

continues; continuité de la fonction composée de deux fonctions continues (sans démonstration).
On admettra sans démonstration le théorème suivant : « si une fonction est continue sur un intervalle, l'image, par la fonction, de cet intervalle est un intervalle ».
Application à une fonction continue et strictement monotone sur un intervalle : existence de la fonction réciproque; monotonie et continuité de cette fonction (on admettra la continuité).

2. *Fonctions numériques d'une variable réelle : limites*

Limite d'une fonction lorsque la variable tend vers un nombre réel donné, vers l'infini. Unicité. Cas particulier des suites.
Limite d'une somme, d'un produit, d'un quotient (sans démonstration).

3. *Fonctions numériques d'une variable réelle : dérivation*

Révision du programme de Première E : fonction linéaire tangente en un point à une fonction donnée; notation différentielle; dérivée en ce point. Fonction dérivée; dérivée d'une somme, d'un produit, d'un quotient de fonctions dérivables. Interprétation géométrique de la dérivée (repère cartésien); équation de la tangente. Définition des dérivées successives.
Dérivée en un point de la composée de deux fonctions dérivables.
Dérivée en un point de la réciproque d'une fonction dérivable et strictement monotone.
On admettra sans démonstration que si une fonction numérique est dérivable sur un intervalle et si sa dérivée est positive ou nulle, elle est croissante au sens large sur cet intervalle.
Comparaison de deux fonctions ayant même fonction dérivée sur un intervalle.
Étude du sens de variation d'une fonction dérivable à l'aide du signe de sa dérivée.
Représentation graphique; exercices simples de recherche d'asymptotes.

4. *Fonctions vectorielles d'une variable réelle*

Application d'une partie de $\mathbb{R}$ dans un espace vectoriel euclidien de dimension finie.
Continuité en un point; limite d'une fonction lorsque la variable tend vers un nombre réel donné, vers l'infini.
Dérivée en un point; si l'espace vectoriel est rapporté à une base, coordonnées, dans cette base, de la dérivée; fonction dérivée.
Dérivée d'une somme de fonctions vectorielles dérivables, du produit d'une fonction vectorielle dérivable par une fonction numérique dérivable.
Dérivée du produit scalaire de deux fonctions vectorielles dérivables. Application à la recherche de tangentes; exemples des coniques et des hélices circulaires.

5. *Cinématique du point*

Mouvement d'un point : application d'un intervalle de $\mathbb{R}$ dans un espace affine euclidien. Trajectoire.
Vecteur-vitesse à un instant donné. Un repère étant choisi, coordonnées du vecteur-vitesse dans ce repère. Norme du vecteur-vitesse.
Vecteur-accélération à un instant donné. Un repère étant choisi, coordonnées du vecteur-accélération dans ce repère.
Étude des mouvements circulaires (vitesse angulaire); étude des mouvements hélicoïdaux uniformes.

IV. Calcul intégral

1. Définition des sommes de Riemann d'une fonction numérique d'une variable réelle sur un intervalle fermé, borné. Existence de l'intégrale pour une fonction monotone; notation $\int_b^a f(t)\,dt$; premières propriétés. On admettra que ces propriétés s'étendent à des fonctions continues, ou monotones par morceaux.
Moyenne d'une telle fonction sur un intervalle fermé, borné. Lien avec la dérivation en des points où la fonction est continue.
Primitives; ensemble des primitives; égalité $\int_a^b f(t)\,dt = \mathrm{F}(b) - \mathrm{F}(a)$, f étant continue sur $[a, b]$ et admettant F pour primitive.
Calcul de primitives; intégration par parties.

2. On énoncera, sans démonstration, les propriétés des aires dont l'existence est admise ici (additivité, unité d'aire...)
Application du calcul intégral à l'évaluation de l'aire de la partie de $\mathbb{R} \times \mathbb{R}$ définie par $a \leqslant x \leqslant b$ $0 \leqslant y \leqslant f(x)$, f étant une fonction positive monotone par morceaux, puis une fonction positive continue.
Extensions à $b < a$ et à une fonction négative.

3.* Applications géométriques, mécaniques, physiques etc. (calcul de volumes, masses, moments d'inertie; vitesse et distance parcourue; intensité et quantité d'électricité; puissance et énergie, etc.).
Valeur efficace d'un phénomène périodique.
(Le paragraphe IV.3 ne fait pas partie — voir Préambule a) — du programme des épreuves de mathématiques du baccalauréat.)

V. Exemples de fonctions d'une variable réelle

Certains résultats de ce chapitre, déjà connus des élèves pourront illustrer les chapitres précédents; il sera opportun de répartir les différentes rubriques de celui-ci entre plusieurs moments de l'année.

1. *Fonction* $x \longmapsto x^n$ ($n \in \mathbb{Z}$); dérivée; primitives.

2. *Fonction* $x \longmapsto x^r$ ($r \in \mathbb{Q}, x > 0$) dérivée; primitives.

3. *Suites arithmétiques et géométriques.* Somme des n premiers termes.

4. *Fonctions circulaires*; dérivées (révision); dérivées et primitives de $x \longmapsto \cos(ax + b)$ et $x \longmapsto \sin(ax + b)$.

5. *Logarithme népérien* (notations Log et ln) : $\operatorname{Log} x = \int_1^x \frac{dt}{t}$ ($x > 0$). Limite, quand la variable positive x tend vers l'infini, de $\operatorname{Log} x$ et de $\frac{\operatorname{Log} x}{x}$. Limite, quand x tend vers 0, de $x \operatorname{Log} x$. Représentation graphique.

6. *Fonction exponentielle* (notation exp).

Propriétés; dérivée; représentation graphique; nombre e; notation e^x; limite de $\frac{e^x}{x}$ quand x tend vers $+\infty$.

7. *Autres fonctions logarithmiques et exponentielles*

Relations entre les fonctions exponentielle et logarithmique de base a et celles de base e.
*Notation e^{ix} pour désigner $\cos x + i \sin x$; ω étant une constante réelle, dérivée de la fonction $x \longmapsto e^{i\omega x}$.

Remarque : l'étude d'exemples de fonctions composées du type logarithmique ou exponentiel sera strictement limitée aux cas où sont en évidence les intervalles sur lesquels la dérivée garde un signe constant et où les indéterminations à lever sont uniquement celles qui ont été énumérées plus haut.

8. *Calcul numérique*

Révision des programmes de Seconde T et Première E.

9. **Équations différentielles*

Recherche des fonctions numériques une ou deux fois dérivables de la variable réelle x vérifiant les équations :
$y' = ay$, a étant une constante réelle,
$y'' + \omega^2 y = 0$, ω étant une constante réelle non nulle (on admettra que les solutions forment un espace vectoriel de dimension 2).
(Le paragraphe V.9 — voir Préambule a) — ne fait pas partie du programme des épreuves de mathématiques du baccalauréat.)

VI. Éléments de géométrie affine et euclidienne

N. B.: Dans ce paragraphe le corps de base est $\mathbb{R}$ et la dimension n est toujours égale à 2 ou 3. Une « transformation d'un ensemble E » est une bijection de E sur lui-même; une application f de E dans lui-même est une involution si $f \circ f$ est l'identité : c'est une transformation de E.

1. Somme directe de deux sous-espaces vectoriels; sous-espaces vectoriels supplémentaires. Application linéaire d'un espace vectoriel E dans un espace vectoriel F : image et noyau. Addition et composition des applications linéaires.
Groupe linéaire. Homothéties vectorielles.

2. Barycentre dans un espace affine. Variété affine. Repère affine. Réduction, dans le cas euclidien, de $f(M) = a\,MA^2 + b\,MB^2 + c\,MC^2$.

3. Application affine d'un espace affine E dans lui-même, application linéaire associée. Exemples : projection parallèle sur un sous-espace affine; involutions affines, leurs points fixes; translations et homothéties.

4. Applications linéaires d'un espace vectoriel euclidien dans lui-même conservant la norme; transformations orthogonales (isométries vectorielles), groupe orthogonal.
Dans le plan vectoriel et dans l'espace vectoriel de dimension trois, éléments fixes des transformations orthogonales involutives (symétries).
Orientation du plan vectoriel euclidien (rappel de la classe de Première).
Étude des rotations vectorielles de l'espace vectoriel euclidien de dimension trois (par définition, une telle rotation est, soit l'identité, soit une transformation orthogonale qui a pour seuls éléments fixes ceux d'une droite vectorielle); on admettra que les rotations vectorielles forment un groupe; orientation de l'espace.
Produit vectoriel, dans l'espace vectoriel euclidien orienté de dimension trois.

5. Définition d'une isométrie de l'espace affine euclidien. Toute isométrie est une bijection affine. Groupe des isométries; sous-groupe des déplacements.
Dans le plan affine euclidien, symétries, translations, rotations : tout déplacement est de l'un de ces deux derniers types.
Dans l'espace affine euclidien de dimension trois, symétries, translations, rotations, vissages; on admettra que tout déplacement est de l'un de ces trois derniers types.
Exemples simples de groupes d'isométries laissant invariant un ensemble donné.

VII. Compléments de géométrie euclidienne plane

1. Angle d'un couple de demi-droites vectorielles (rappel de Première); groupe $\mathcal{A}$ des angles de demi-droites.
Angle d'un couple de droites vectorielles (ensemble des deux rotations vectorielles transformant la première en la seconde); groupe $\mathcal{A}'$ des angles de droites. Homomorphisme canonique $\mathcal{A} \longrightarrow \mathcal{A}'$; son noyau. Isomorphisme $\mathcal{A}' \longrightarrow \mathcal{A}$ déduit de l'homomorphisme $\alpha \longmapsto \alpha + \alpha$ de $\mathcal{A}$ sur $\mathcal{A}$.
Condition, en termes d'angles de droites, pour que quatre points soient cocycliques.

2. Similitudes planes (c'est-à-dire applications du plan dans lui-même conservant les rapports de distances). Représentation par les formules $z' = az + b$ ou $z' = a\bar{z} + b$ lorsque l'on a identifié le plan à $\mathbb{C}$ grâce au choix d'un repère orthonormé.
Points fixes des similitudes. Groupe des similitudes du plan et sous-groupes remarquables.

3. Étude des courbes représentées, dans un repère orthonormé, par des équations de la forme $ax^2 + by^2 + 2cx + 2dy + e = 0$ ($|a| + |b| \neq 0$).
Différentes formes de ces courbes; existence d'axes ou de centres de symétrie, d'asymptotes. Équations réduites : ellipse, hyperbole, parabole. Existence de la tangente. Équation de l'hyperbole rapportée à ses asymptotes.

4. Géométrie descriptive. Les questions énumérées ci-dessous seront avantageusement étudiées en liaison avec le cours de géométrie de cette classe et de la classe antérieure; elles serviront utilement à son illustration.
Rotation autour d'un axe vertical, ou de bout.
Rabattement d'un plan sur un plan horizontal ou frontal.
Distance de deux points, d'un point à une droite, d'un point à un plan; angle de deux droites.
Projection d'un cercle : épure.
Représentation d'un cylindre de révolution, d'un cône de révolution dont une base circulaire est dans le plan horizontal de projection.
Construction par points et tangentes de la projection horizontale (resp. frontale) de l'intersection d'une telle surface par un plan de bout (resp. vertical).
Représentation de l'hélice circulaire droite tracée sur un cylindre de révolution d'axe vertical.

VIII. Probabilités sur un ensemble fini

1. Espaces probabilisés finis $(\Omega, \mathfrak{B}(\Omega), p)$.
Applications mesurables (ou variables aléatoires); probabilité, image, fonction de répartition d'une variable aléatoire réelle.
Couple de variables aléatoires réelles, loi du couple. Lois marginales.
Couple indépendant. Système de n variables aléatoires indépendantes.

2. Espérance mathématique d'une variable aléatoire à valeurs dans $\mathbb{R}$ ou $\mathbb{R}^2$. Espérance mathématique de la somme des deux variables aléatoires réelles d'un couple, du produit dans le cas d'un couple indépendant.
Variance, écart-type d'une variable aléatoire réelle.

3. Inégalité de Bienaymé-Tchebycheff. Épreuves répétées; loi faible des grands nombres.

1| Entiers naturels.

La section I de ce chapitre est consacrée à la présentation des entiers naturels. Conformément au programme nous avons admis les principales propriétés de $(\mathbb{N}, +, \times, \leqslant)$.

Nous avons ensuite effectué une révision de certains problèmes de dénombrement étudiés en Première, car, d'une part, ils fournissent des exemples très instructifs de raisonnement par récurrence, et, d'autre part, certains de ces résultats nous seront très utiles par la suite (formule du binôme, probabilités).

Enfin la section II présente la division euclidienne dans $\mathbb{N}$ *et son application à l'étude des systèmes de numération.*

Nous commencerons par donner des compléments sur les lois de composition interne et sur les relations d'ordre; cela nous permettra de ne pas rompre l'exposé des propriétés de $\mathbb{N}$ *par l'introduction de nouvelles notions.*

1.1 ÉLÉMENTS RÉGULIERS POUR UNE LOI DE COMPOSITION INTERNE

Considérons une loi de composition interne définie sur E; nous la noterons T.
L'unicité du composé $a \top b$ de a et b de E entraîne que, quels que soient a, b, c de E, on a

$$(a = b) \Longrightarrow (c \top a = c \top b)$$
$$(a = b) \Longrightarrow (a \top c = b \top c).$$

En revanche les implications réciproques de ces deux implications ne sont pas toujours vraies.

EXEMPLES

1. Dans $(\mathcal{P}(E), \cup)$ on peut trouver des éléments A et B tels que $E \cup A = E \cup B$ et $A \neq B$, car $E \cup X = E$ pour tout X.
   En revanche quels que soient A et B de $\mathcal{P}(E)$ on a
   $$(\varnothing \cup A = \varnothing \cup B) \Longrightarrow (A = B)$$

2. De même dans $(\mathcal{P}(E), \cap)$ on peut trouver A et B tels que $\varnothing \cap A = \varnothing \cap B$ et $A \neq B$, car $\varnothing \cap X = \varnothing$ pour tout X.
   En revanche quels que soient A et B de $\mathcal{P}(E)$ on a
   $$(E \cap A = E \cap B) \Longrightarrow (A = B).$$

Ces exemples légitiment les définitions suivantes :

Définitions.

On dit que a est un élément **régulier à gauche** dans (E, T) si et seulement si, quels que soient x et y de E, on a

$$(a \mathrel{T} x = a \mathrel{T} y) \Longrightarrow (x = y);$$

de même a est **régulier à droite** si et seulement si, quels que soient x et y de E, on a

$$(x \mathrel{T} a = y \mathrel{T} a) \Longrightarrow (x = y);$$

si a est régulier à la fois à droite et à gauche on dit que a est **régulier.**

Naturellement si la loi T est *commutative* ces trois notions se confondent, on parlera uniquement dans ce cas d'éléments réguliers.

D'après les exemples ci-dessus, dans $(\mathfrak{P}(E), \cup)$ $\varnothing$ est régulier et E n'est pas régulier; les résultats sont inversés dans $(\mathfrak{P}(E), \cap)$.

EXERCICES

1. Une partie propre de E est-elle un élément régulier dans $(\mathfrak{P}(E), \cup)$? dans $(\mathfrak{P}(E), \cap)$?
2. On considère (E, T) et les deux applications γ_a et δ_a appelées respectivement *translation à gauche* et *translation à droite* relatives à a de E et définies par

$$\gamma_a : E \longrightarrow E \qquad \delta_a : E \longrightarrow E$$
$$x \longmapsto a \mathrel{T} x \qquad a \longmapsto x \mathrel{T} a$$

Démontrer que a est régulier à gauche (resp. à droite) si et seulement si γ_a (resp. δ_a) est injective.

1.2 RELATIONS D'ORDRE (RÉVISIONS ET COMPLÉMENTS)

a) Relation d'ordre (révision).

Une relation binaire $\mathcal{R}$ définie sur un ensemble E est une **relation d'ordre** si et seulement si $\mathcal{R}$ possède les propriétés suivantes :

1. Quel que soit x de E on a $\mathcal{R}(x, x)$.
2. Quels que soient x et y de E on a

$$[\mathcal{R}(x, y) \quad \text{et} \quad \mathcal{R}(y, x)] \Longrightarrow (x = y).$$

3. Quels que soient x, y, z de E on a

$$[\mathcal{R}(x, y) \quad \text{et} \quad \mathcal{R}(y, z)] \Longrightarrow \mathcal{R}(x, z).$$

On voit immédiatement que la conjonction de (1) et (2) est équivalente à :

2′. Quels que soient x et y de E on a

$$[\mathcal{R}(x, y) \quad \text{et} \quad \mathcal{R}(y, x)] \Longleftrightarrow (x = y).$$

Les propriétés 1 et 3 s'énoncent respectivement : $\mathcal{R}$ est *réflexive* et $\mathcal{R}$ est *transitive*.

Dans la première édition de notre livre de Seconde nous avons appelé antisymétrique toute relation vérifiant (2′). La plupart des lecteurs semblent préférer pour relation antisymétrique la définition (2).

Ce qu'il faut bien voir, c'est que la seule notion importante est celle de **relation d'ordre :** les relations qui ne posséderaient que (2) ou (2′) ne se rencontrent pratiquement jamais. Aussi nous ne voyons aucun inconvénient à appeler désormais relation *antisymétrique* toute relation possédant la propriété (2).

S'il n'y a pas de signe spécifique pour noter une relation d'ordre (par exemple $\leqslant$ dans $\mathbb{R}$, $\subset$ dans $\mathfrak{P}(E)$) on utilisera le symbole $\preccurlyeq$.

On note $(E, \preccurlyeq)$ l'ensemble E muni de la relation d'ordre $\preccurlyeq$; on dit que E est *ordonné* par cette relation.

La relation réciproque d'une relation d'ordre notée $\preccurlyeq$ se notera $\succcurlyeq$.
Quels que soient x et y de E

$$(x \preccurlyeq y \text{ et } x \neq y) \quad \text{se note} \quad x \prec y,$$
$$(x \succcurlyeq y \text{ et } x \neq y) \quad \text{se note} \quad x \succ y.$$

Ces relations, notées $\prec$ et $\succ$, réciproques l'une de l'autre, *ne sont pas des relations d'ordre* (elles ne sont pas réflexives); c'est, par conséquent, par *abus de langage* que l'on dit que ce sont des relations d'*ordre strict*.
Enfin si *quels que soient x et y* de E on a

$$x \preccurlyeq y \quad \textit{ou} \quad y \preccurlyeq x,$$

on dit que la relation notée $\preccurlyeq$ est une *relation d'ordre total.*
Si cette propriété n'est pas vérifiée, on dit que l'ordre est *partiel;* ce qui signifie donc qu'*il existe x et y de* E tel que ($x \preccurlyeq y$ ou $y \preccurlyeq x$) soit faux.

b) Majorants (resp. minorants) d'une partie d'un ensemble ordonné.

Définitions.

Soit F une partie non vide de E ordonné. On dit que a de E est un **majorant** de F si et seulement si

$$(\forall\, x \in F) \qquad x \preccurlyeq a,$$

et un **minorant** de F si et seulement si

$$(\forall\, x \in F) \qquad a \preccurlyeq x.$$

EXEMPLES

1. Soit A et B deux parties d'un ensemble E telles que $A \subset B$ et $A \neq B$ considérons
$$\mathfrak{Q} = \{X \in \mathfrak{P}(E) \mid A \subset X \subset B\}$$
Toute partie de A est un minorant de $\mathfrak{Q}$ (pour l'inclusion). Ainsi si $A = \{a, b\}$ avec $a \neq b$, $\varnothing$, $\{a\}$, $\{b\}$, A sont des minorants de $\mathfrak{Q}$.
De même toute partie E incluant B est un majorant de $\mathfrak{Q}$.
2. Nous le reverrons ci-dessous, mais vous savez qu'il n'existe pas d'entier naturel plus grand que tous les autres; donc pour l'ordre naturel des entiers, $\mathbb{N}$ n'admet pas de majorant dans $\mathbb{N}$.
De même $\mathbb{Z}$ n'admet ni majorant, ni minorant dans $\mathbb{Z}$.

Les exemples ci-dessus montrent que s'il existe un majorant a de $F \subset E$ ce majorant n'est pas forcément unique; en particulier la transitivité de la relation d'ordre montre que tout a' de E tel que $a \preccurlyeq a'$ (a étant un majorant de F) est encore un majorant de F
On a des résultats analogues pour la notion de minorant.
D'autre part le fait que, pour F, partie de E ordonné, il existe ou il n'existe pas de majorant ou de minorant légitime les définitions suivantes :

Définitions.

On dit qu'une partie F de E ordonné est **majorée** (resp. **minorée**) si et seulement si F admet au moins un majorant (resp. minorant). On dit que F est **bornée** si et seulement si elle est à la fois minorée et majorée.

Ainsi l'ensemble $\mathfrak{Q}$ (ex. 1 ci-dessus) est borné (pour la relation d'inclusion).

c) Plus grand (resp. petit) élément d'une partie d'un ensemble ordonné.

Soit F une partie d'un ensemble ordonné E; supposons qu'il existe des majorants a, a'... de F, *appartenant à* F; on aura donc $a \preccurlyeq a'$ puisque a' est un majorant de F et que $a \in F$ et de même $a' \preccurlyeq a$, donc $a = a'$.

On obtient le même résultat pour les minorants de F appartenant à F.

Théorème et définition.

S'il existe un majorant (resp. minorant) de F, partie de E ordonné, appartenant à F, cet élément est unique. Il est appelé **plus grand** (resp. **plus petit**) **élément** de F.

Comme les exemples suivants le prouvent toute partie majorée (resp. minorée) de E ne possède pas forcément un plus grand (resp. plus petit) élément.

EXEMPLES

3. Reprenons l'exemple 1 ci-dessus : A est le plus petit élément de $\mathfrak{Q}$ et B le plus grand. Mais si nous considérons avec les mêmes notations
$$\mathfrak{Q}' = \{X \in \mathfrak{T}(E) \mid A \subset X \subset B \text{ et } X \neq A\}$$
$\mathfrak{Q}'$ a un plus grand élément B mais pas de plus petit élément.

4. Vous connaissez l'ensemble $\mathbb{Q}$ des rationnels, nous le retrouverons dans le chapitre 3. Considérons $E = [0, 1]$, $E' =]0, 1[$ intervalles respectivement fermé et ouvert de $\mathbb{Q}$ ordonné par l'ordre total noté $\leqslant$. Ces intervalles sont bornés.
L'intervalle E a un plus petit élément 0 et un plus grand élément 1.
En revanche E' n'a ni plus grand ni plus petit élément; on voit par exemple que si r était le plus petit élément de $]0, 1[$ on aurait $\frac{1}{2} r \in]0, 1[$ et $\frac{1}{2} r < r$ et r ne serait pas le plus petit élément de $]0, 1[$.

d) Borne supérieure (resp. inférieure) d'une partie majorée (resp. minorée) d'un ensemble ordonné.

Soit F une partie non vide majorée d'un ensemble ordonné; donc l'*ensemble* M *des majorants* de F n'est pas vide; s'il existe dans M *un plus petit élément* a_0 il est appelé **borne supérieure** de F; on écrit
$$\sup F = a_0.$$
De même si l'*ensemble des minorants* de F, partie non vide minorée de E, a un plus grand élément a_0, il est appelé **borne inférieure** de F; on écrit
$$\inf F = a_0.$$

EXEMPLES

5. Reprenons les exemples 1 et 3 ci-dessus on voit que
$$\inf \mathfrak{Q} = \inf \mathfrak{Q}' = A$$
$$\sup \mathfrak{Q} = \sup \mathfrak{Q}' = B$$

6. Reprenons l'exemple 4 ci-dessus on voit que
$$\inf [0, 1] = \inf]0, 1[= 0$$
$$\sup [0, 1] = \sup]0, 1[= 1$$

Ces notions de borne inférieure ou supérieure joueront un rôle fondamental dans l'étude des nombres réels (chap. 3).

Notons cependant tout de suite le résultat suivant. Si a et b sont deux éléments quelconques de E **totalement ordonné** on a $a \preccurlyeq b$ ou $b \preccurlyeq a$; supposons $a \preccurlyeq b$; l'ensemble des majorants de $\{a, b\}$ est l'ensemble des x de E tels que $b \preccurlyeq x$ le plus petit d'entre eux est b; donc b est la borne supérieure de $\{a, b\}$; on verrait de même que a est la borne inférieure de $\{a, b\}$.

Donc si, dans E totalement ordonné, on a $a \preccurlyeq b$, $\{a, b\}$ a une borne inférieure a et une borne supérieure b on écrit
$$\inf (a, b) = a \quad , \quad \sup (a, b) = b.$$
(On commet ainsi un abus de notation car on devrait écrire
$$\inf \{a, b\} = a \quad \text{et} \quad \sup \{a, b\} = b)$$

I. Entiers naturels. Ensembles finis

1.3 ENSEMBLE $\mathbb{N}$ DES ENTIERS NATURELS

Dans ce paragraphe nous ne cherchons pas à construire $\mathbb{N}$ ni à démontrer les principales propriétés de $(\mathbb{N}, +, \times, \leqslant)$. Les lecteurs intéressés par ces questions trouveront à l'annexe B les grandes lignes de l'une des méthodes de construction de $\mathbb{N}$. En particulier les propriétés que nous allons énoncer ne sont pas toutes indépendantes, en ce sens que certaines d'entre elles pourraient se déduire de certaines autres; nous ne chercherons pas à faire une telle distinction qui nous conduirait, si elle était bien faite, à une définition axiomatique de $\mathbb{N}$. Toutefois, pour alléger l'exposé, nous présenterons sous forme d'exercices les conséquences absolument immédiates des propriétés énoncées.

Nous **admettrons** qu'il existe un ensemble, noté $\mathbb{N}$, d'éléments appelés **entiers naturels** et possédant les propriétés suivantes :

a) Propriétés de $(\mathbb{N}, +, \times)$.

Il existe dans $\mathbb{N}$ une **addition** et une **multiplication** telles que :

1. L'*addition* est *associative*, *commutative*, possède un *élément neutre* « zéro » noté 0, et tout élément de $\mathbb{N}$ est *régulier* pour l'addition.

On pose $$\mathbb{N}^* = \mathbb{N} - \{0\}.$$

2. La *multiplication* est *associative*, *commutative*, possède un *élément neutre* « un » noté 1, et tout élément de $\mathbb{N}^*$ est *régulier* pour la multiplication.
3. La multiplication est *distributive* par rapport à l'addition.

EXERCICES

1. Étant donnés a et b de $\mathbb{N}$, s'il existe x de $\mathbb{N}$ tel que $a + x = b$, démontrer que x est unique; si x existe, on le note $b - a$; on a donc par définition
$$a + (b - a) = b.$$
2. Si $b - a$ existe, démontrer que, quel que soit c de $\mathbb{N}$, $cb - ca$ existe et que l'on a
$$c(b - a) = cb - ca.$$
3. Démontrer que, pour tout x de $\mathbb{N}$, on a
$$0\,x = 0.$$
En déduire que 0 n'est pas régulier pour la multiplication et que, par conséquent, $0 \neq 1$.

b) Ordre naturel sur $\mathbb{N}$.

1. La relation « *il existe x de $\mathbb{N}$ tel que $b = a + x$* » est une relation d'**ordre total** définie sur $\mathbb{N}$; on la note $a \leqslant b$. Elle est appelée relation d'ordre naturel sur $\mathbb{N}$.
La relation « $a \leqslant b$ et $a \neq b$ » se note $a < b$. De plus $a \geqslant b$ signifie $b \leqslant a$ et $a > b$ signifie $b < a$.
2. La relation d'ordre notée $\leqslant$ est *compatible avec l'addition* c'est-à-dire que, quels que soient a, b, c de $\mathbb{N}$, on a
$$(a \leqslant b) \Longrightarrow a + c \leqslant b + c.$$

3. Pour la relation d'ordre naturel sur $\mathbb{N}$ on a de plus les propriétés suivantes :

- *Toute partie non vide de* $\mathbb{N}$ *a un plus petit élément.* Zéro est le plus petit élément de $\mathbb{N}$; donc, pour tout x de $\mathbb{N}$, on a $0 \leqslant x$.
- *Toute partie non vide majorée de* $\mathbb{N}$ *a un plus grand élément.* $\mathbb{N}$ n'a pas de plus grand élément.

EXERCICES

4. Démontrer que, quels que soient a, b, c de $\mathbb{N}$, on a

$$(a < b) \Longrightarrow (a + c < b + c);$$

en déduire que, quels que soient a, b, c de $\mathbb{N}$, on a

$$(a < b) \Longleftrightarrow (a + c < b + c),$$
$$(a \leqslant b) \Longleftrightarrow (a + c \leqslant b + c).$$

5. Démontrer que, pour tout x de $\mathbb{N}^*$, on a $0 < x$; en particulier on a $0 < 1$.

6. Si $c \in \mathbb{N}^*$ démontrer que, quels que soient a et b de $\mathbb{N}$, on a

$$(a \leqslant b) \Longleftrightarrow (ac \leqslant bc),$$
$$(a < b) \Longleftrightarrow (ac < bc).$$

(On se rappellera que $a \leqslant b$ signifie : il existe x de $\mathbb{N}$ tel que $b = a + x$).

7. Démontrer que, quels que soient a et b de $\mathbb{N}$, on a

$$(ab = 0) \Longleftrightarrow (a = 0 \quad \text{ou} \quad b = 0).$$

1.4 INTERVALLES DE $\mathbb{N}$

a) Définition.

Quels que soient les entiers naturels a et b, vérifiant $a \leqslant b$, on appelle **intervalle** de $\mathbb{N}$ l'un quelconque des sous-ensembles de $\mathbb{N}$ suivants :

$$[a\,,\,b] = \{x \in \mathbb{N} \mid a \leqslant x \leqslant b\},$$
$$]a\,,\,b[= \{x \in \mathbb{N} \mid a < x < b\},$$
$$[a\,,\,b[= \{x \in \mathbb{N} \mid a \leqslant x < b\},$$
$$]a\,,\,b] = \{x \in \mathbb{N} \mid a < x \leqslant b\},$$
$$[a\,,\,+\infty[= \{x \in \mathbb{N} \mid a \leqslant x\},$$
$$]a\,,\,+\infty[= \{x \in \mathbb{N} \mid a < x\}.$$

Remarquons que $\mathbb{N} = [0\,,\,+\infty[$.

b) Structure des intervalles de $\mathbb{N}$.

Nous allons voir que les intervalles non vides de $\mathbb{N}$ se ramènent à l'un des types suivants $[a\,,\,b]$ où $a \leqslant b$, ou $[a\,,\,+\infty[$.
Nous utiliserons pour cela le lemme suivant :

Lemme.
L'intervalle $]0\,,\,1[$ est vide.

En effet supposons $]0\,,\,1[$ non vide; il admet alors un plus petit élément α (cf. § 1.3 b); on a $0 < \alpha < 1$, d'où $0 < \alpha^2 < \alpha$ et par conséquent $0 < \alpha^2 < 1$; donc α^2 serait un élément de $]0\,,\,1[$ strictement inférieur à α, plus petit élément de $]0\,,\,1[$; c'est impossible; donc notre hypothèse est fausse et par conséquent $]0\,,\,1[$ est vide. De même on voit que $]n\,,\,n+1[$ est vide quel que soit l'entier n.

Il résulte du lemme que pour tout x de $\mathbb{N}$ on a

$$(0 < x) \iff (1 \leqslant x)$$

et plus généralement, comme $]n\,,\,n+1[$ est vide, on peut énoncer

Corollaire 1.

Quels que soient x et n de $\mathbb{N}$

$$(n < x) \iff (n+1 \leqslant x).$$

Étudions maintenant $]a\,,\,b[$ où $a \leqslant b$; on constate que si $a = b$ ou $a+1 = b$ cet intervalle est vide; si $a+1 < b$ on voit immédiatement que $]a\,,\,b[= [a+1\,,\,b-1]$.
De même $[a\,,\,b[$ et $]a\,,\,b]$ sont vides si $a = b$; si $a < b$ on voit que l'on aura $[a\,,\,b[= [a\,,\,b-1]$ et $]a\,,\,b] = [a+1\,,\,b]$. Enfin $]a\,,+\infty[= [a+1\,,+\infty[$. Par conséquent tout intervalle non vide de $\mathbb{N}$ est de la forme $[a\,,\,b]$ ou $[a\,,+\infty[$; le premier est majoré, le deuxième n'est pas majoré; concluons :

Corollaire 2.

Tout intervalle **non vide** de $\mathbb{N}$ est de la forme
$[a\,,\,b]$ s'il est majoré,
$[a\,,+\infty[$ s'il n'est pas majoré.

REMARQUE

Nous avons vu que, pour tout n de $\mathbb{N}$, $]n\,,\,n+1[= \varnothing$; on dit que tout entier naturel n a un *successeur* $n+1$.
De même si $n \in \mathbb{N}^*$, on a $0 < n$, donc $1 \leqslant n$; $n-1$ existe et $]n-1\,,\,n[= \varnothing$; on dit que tout entier naturel n de $\mathbb{N}^*$ a un *prédécesseur* $n-1$.

1.5 RAISONNEMENT PAR RÉCURRENCE

Soit X une partie de $\mathbb{N}$ vérifiant les deux propriétés suivantes :
i. $0 \in X$
ii. $(\forall\, x \in X) \quad x+1 \in X$.
Nous allons montrer que $X = \mathbb{N}$; il revient au même de montrer que $Y = \mathbb{N} - X = \varnothing$.
Supposons $Y \neq \varnothing$, cette partie de $\mathbb{N}$ a alors un plus petit élément p (cf. § 1.3 b). Cet entier naturel p est non nul, puisque $0 \in X$; donc $p \geqslant 1$ (cf § 1.4 b); il existe donc un entier naturel $p' = p - 1$ (cf § 1.3 a); on a $p' < p$ donc $p' \notin Y$ puisque p est supposé être le plus petit élément de Y; par conséquent $p' \in X$ et $p = p' + 1 \in X$ d'après l'hypothèse *ii*); p ne pouvant appartenir à X et Y, parties complémentaires de $\mathbb{N}$ n'existe pas : notre hypothèse $Y \neq \varnothing$ est donc fausse. Concluons :

Théorème.

Toute partie X de $\mathbb{N}$ telle que
i. $0 \in X$.
ii. $(\forall\, x \in X) \quad x+1 \in X$
est identique à $\mathbb{N}$.

Nous pouvons énoncer ce résultat en utilisant, au lieu de la notion de *partie* de $\mathbb{N}$, celle de *propriété ayant un sens sur* $\mathbb{N}$ (on dit aussi *définie* sur $\mathbb{N}$).
Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$ posons

$$X = \{x \in \mathbb{N} \mid \mathcal{P}(x)\};$$

la partie X possédera les deux propriétés de l'hypothèse du théorème précédent si et seulement si on a à la fois $\mathcal{P}(0)$ et

$$(\forall\, n \in \mathbb{N}) \quad [\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)]$$

Corollaire.

Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$; si on a
i. $\mathcal{P}(0)$
ii. $(\forall\, n \in \mathbb{N}) \quad [\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)]$
alors $\mathcal{P}(n)$ est vrai pour tout entier naturel n.

Nous rencontrerons beaucoup d'exemples de raisonnement par récurrence par la suite; voici tout de suite un exemple :

EXEMPLE 1

Soit $\mathcal{P}$ la propriété *définie* sur $\mathbb{N}$ par

« pour tout $n \in \mathbb{N}$, l'entier $n^3 - n$ est divisible par 3 ».

(On dit qu'un entier naturel a est divisible par 3 si et seulement s'il existe un entier naturel k tel que $a = 3k$).
$\mathcal{P}(0)$ est vrai car 0 est divisible par 3.
Pour démontrer que pour tout n de $\mathbb{N}$ on a

$$\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$$

nous démontrerons que, si $\mathcal{P}(n)$ est vrai, alors $\mathcal{P}(n+1)$ est vrai.
Supposons $\mathcal{P}(n)$ vrai (on dit que c'est l'*hypothèse de la récurrence* considérée); il existe donc $k \in \mathbb{N}$ tel que

$$n^3 - n = 3k.$$

On a, d'autre part

$$\begin{aligned}(n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - (n+1) \\ &= (n^3 - n) + 3(n^2 + n) = 3k + 3(n^2 + n) \\ &= 3(k + n^2 + n)\end{aligned}$$

donc si $\mathcal{P}(n)$ est vrai il en est de même de $\mathcal{P}(n+1)$.
Donc pour tout n de $\mathbb{N}$, $\mathcal{P}(n)$ est un énoncé vrai.

Dans l'étude ci-dessus on dit que l'on a effectué une *récurrence sur* $\mathbb{N}$; on peut faire également des récurrences sur des intervalles I de $\mathbb{N}$ distincts de $\mathbb{N}$. Vous démontrerez exactement comme ci-dessus les résultats suivants:

Récurrence à partir de l'entier naturel a. Soit $\mathcal{P}$ une propriété définie sur l'intervalle $[a\,,+\infty[$ de $\mathbb{N}$; si on a
i. $\mathcal{P}(a)$.
ii. $(\forall\, n \in [a\,,+\infty[) \quad (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))$
alors $\mathcal{P}(n)$ est vrai pour tout n de $[a\,,+\infty[$.

Récurrence sur $[a, b]$ où $a < b$. Soit $\mathcal{P}$ une propriété définie sur l'intervalle $[a, b]$ de $\mathbb{N}$ $(a < b)$; si on a
i. $\mathcal{P}(a)$
ii. $\forall\, n \in [a, b-1] \quad (\mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1))$
alors $\mathcal{P}(n)$ est vrai pour tout n de $[a, b]$.

EXEMPLE 2

Démontrer que la somme $f(n)$ des entiers naturels impairs x tels que

$$1 \leqslant x \leqslant 2n - 1 \text{ est } n^2.$$

Cette propriété $\mathcal{P}$ est définie pour tout $n \geqslant 1$ c'est-à-dire sur $\mathbb{N}^*$.
$\mathcal{P}(1)$ signifie $f(1) = 1 = 1^2$, donc $\mathcal{P}(1)$ est vrai.

Supposons $f(n) = n^2$; $f(n+1)$ est la somme des entiers impairs de 1 à $2(n+1) - 1 = 2n + 1$;
or $]2n - 1\ ,\ 2n[= \varnothing$, $]2n\ ,\ 2n + 1[= \varnothing$ et $2n$ est pair donc

$$f(n+1) = f(n) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2$$

Pour tout $n \in \mathbb{N}^*$, $\mathfrak{P}(n)$ implique $\mathfrak{P}(n+1)$. Conclusion : $\mathfrak{P}(n)$ est vrai pour tout n de $\mathbb{N}^*$.

REMARQUE

Supposons que l'on ait simplement dit « Calculer la somme $f(n)$ des entiers impairs x tels que $1 \leqslant x \leqslant 2n - 1$ ».
Avant de pouvoir faire le raisonnement par récurrence, il faut *expliciter la propriété* $\mathfrak{P}$; ici les calculs suivants

$$f(1) = 1\ ,\ f(2) = 1 + 3 = 4\ ,\ f(3) = 1 + 3 + 5 = 9\ldots$$

suggère l'énoncé plausible de $\mathfrak{P}$. Ce n'est pas toujours aussi simple, comme le montre l'exercice suivant. Mais insistons : le *raisonnement par récurrence ne commence que lorsque la propriété à démontrer est explicitée.*

EXERCICE

Calculer la somme $g(n)$ des cubes des entiers x tels que $0 \leqslant x \leqslant n$.

1.6 ENSEMBLES FINIS ET ENSEMBLES INFINIS. CARDINAL D'UN ENSEMBLE FINI. APPLICATIONS

Nous allons admettre les propriétés énoncées dans le sous-paragraphe a); *elles sont démontrées dans l'annexe B à la fin du volume. Les lecteurs ayant étudié cette annexe B sont donc dispensés de lire ce sous-paragraphe* a).

a) Ensemble fini. Cardinal d'un ensemble fini.

Soit deux ensembles E et F tels qu'il existe une bijection f de E sur F; on caractérise cette situation en disant que E est équipotent à F et on écrit

$$\mathrm{E} \text{ eq } \mathrm{F}.$$

Tout ensemble est équipotent à lui-même, il suffit de considérer la bijection $f = \mathrm{Id}_{\mathrm{E}}$.
S'il existe une bijection f de E sur F, il existe une bijection de F sur E, à savoir f^{-1}; donc si E est équipotent à F, alors F est équipotent à E; nous dirons simplement que E et F sont des **ensembles équipotents.**
Enfin si E et F sont équipotents, de même que F et G, nous avons le schéma

$$\mathrm{E} \xrightarrow{f} \mathrm{F} \xrightarrow{g} \mathrm{G},$$

où f et g sont des bijections : il en résulte que $g \circ f$ est une bijection de E sur G; donc E et G sont équipotents.

Définition.

On dit qu'un ensemble E est **finie** s'il est vide ou bien s'il existe un entier naturel $n \geqslant 1$ tel que E soit équipotent à l'intervalle $[1, n]$ de $\mathbb{N}$.
Tout ensemble qui n'est pas fini est dit **infini.**

Nous **admettrons** le résultat suivant :

S'il existe une bijection de E sur $[1\ ,\ n]$ $(n \geqslant 1)$ et une bijection de E sur $[1\ ,\ p]$ $(p \geqslant 1)$, alors $n = p$.

Cet entier naturel unique est appelé **cardinal de l'ensemble fini E.** On écrit

$$\text{card } E = n.$$

On complète cette définition en posant

$$\text{card } \varnothing = 0.$$

On voit donc que card $\{a\} = 1$, card $\{a, b\} = 2$ si et seulement si $a \neq b$ etc.
On voit également que *tous* les ensembles équipotents à E, de cardinal n, sont finis et ont même cardinal. D'un point de vue intuitif le cardinal d'un ensemble fini est le « nombre de ses éléments ».
Nous **admettrons** les résultats suivants :

---

1. Si E est fini, alors toute partie F de E est finie et on a card F $\leqslant$ card E.
   Si de plus F $\neq$ E, on a card F $<$ card E.
2. Si E et F sont finis, alors E $\cup$ F est fini.
   Si de plus E $\cap$ F $= \varnothing$, alors card(E $\cup$ F) = card E + card F.

---

b) Conséquences de ces propriétés.

La propriété 1 entraîne immédiatement le résultat suivant :

---

3. Pour tout ensemble fini E et tout ensemble F on a
   $$(F \subset E \text{ et card } F = \text{card } E) \Longrightarrow (F = E).$$

La propriété 1 entraîne également (car E $\cap$ F $\subset$ E) :

---

4. Si E est fini, alors E $\cap$ F est fini.

Soit deux ensembles E et F on a

(1) $\qquad E \cup F = E \cup (F - E) \quad \text{avec} \quad E \cap (F - E) = \varnothing.$

Rappelons que F — E est l'ensemble des éléments de F n'appartenant pas à E; on a donc

$$F - E = \complement_F (E \cap F)$$

d'où

(2) $\qquad F = (F - E) \cup (E \cap F) \quad \text{avec} \quad (F - E) \cap (E \cap F) = \varnothing.$

Si E et F sont finis les relations (1) et (2) nous permettent d'écrire, grâce à la propriété 2 ci-dessus,

(1′) $\qquad \text{card } (E \cup F) = \text{card } E + \text{card } (F - E),$
(2′) $\qquad \text{card } F = \text{card } (F - E) + \text{card } (E \cap F);$

d'où

---

5. Quels que soient les ensembles finis E et F on a

$$\boxed{\text{card } (E \cup F) + \text{card } (E \cap F) = \text{card } E + \text{card } F}$$

Soient des ensembles *finis* $F_1, F_2 \ldots F_n$ $(n \geqslant 1)$ *deux à deux disjoints;* considérons la propriété $\mathcal{S}$ *définie* pour tout k de $[1, n]$ par « $F_1 \cup F_2 \ldots \cup F_k$ est fini et card $(F_1 \cup F_2 \ldots \cup F_k) = \text{card } F_1 + \text{card } F_2 + \ldots + \text{card } F_k$ ».

L'énoncé $\mathfrak{P}(1)$ est vrai.
D'autre part pour tout k de $[1, n-1]$ on a

$$F_1 \cup F_2 \ldots \cup F_{k+1} = (F_1 \cup F_2 \ldots \cup F_k) \cup F_{k+1}$$

et

$$F_{k+1} \cap (F_1 \cap F_2 \ldots \cap F_k) = \varnothing.$$

Donc si $\mathfrak{P}(k)$ est vrai, il en est de même de $\mathfrak{P}(k+1)$. Donc $\mathfrak{P}(k)$ est vrai pour tout k de $[1, n]$. En particulier $\mathfrak{P}(n)$ est vrai. Concluons :

---

6. Quels que soient les ensembles finis $F_1, F_2, \ldots, F_n$ $(n \geqslant 1)$, *deux à deux disjoints*, $F_1 \cup F_2 \ldots \cup F_n$ est fini et on a

$$\text{card}\,(F_1 \cup F_2 \ldots \cup F_n) = \text{card}\,F_1 + \text{card}\,F_2 + \ldots + \text{card}\,F_n.$$

Ceci s'applique en particulier lorsque $F_1, F_2, \ldots, F_n$ sont les éléments d'une **partition** d'un ensemble fini E; on a alors

$$\text{card}\,E = \text{card}\,F_1 + \text{card}\,F_2 + \ldots + \text{card}\,F_n.$$

c) Parties finies et parties majorées de $\mathbb{N}$.

Montrons d'abord que tout intervalle $[a, b]$ de $\mathbb{N}$ $(a \leqslant b)$ est fini et cherchons son cardinal. Il existe un entier naturel unique c tel que $c + a = b$, on a $c = b - a$. D'autre part quel que soit x de $\mathbb{N}$ on a

$$(0 \leqslant x \leqslant c) \iff (a \leqslant x + a \leqslant b).$$

Donc l'application

$$\begin{array}{ccc} [0, c] & \longrightarrow & [a, b] \\ x & \longmapsto & x + a \end{array}$$

est une bijection.
Il en résulte que $[0, c]$ est équipotent à $[1, c+1]$ et que $\text{card}\,[0, c] = c + 1$; on en déduit immédiatement

Théorème.
Quels que soient les entiers naturels a et b tels que $a \leqslant b$, l'intervalle $[a, b]$ de $\mathbb{N}$ est fini et on a

$$\text{card}\,[a, b] = b - a + 1.$$

Soit F une *partie finie non vide* de $\mathbb{N}$ nous allons montrer que F est majorée; il nous suffit de montrer que F a un plus grand élément.
Raisonnons par récurrence sur le cardinal $n \geqslant 1$ de F. La propriété $\mathfrak{P}$ est *définie* pour tout n de $\mathbb{N}^*$ par : « *Toute partie de* $\mathbb{N}$ *ayant* n *éléments a un plus grand élément.* »
$\mathfrak{P}(1)$ est un énoncé vrai.
Supposons $\mathfrak{P}(n)$ vrai. Si F a $n+1$ éléments il existe une bijection f de $[1, n+1]$ sur F donc

$$F = \{f(1), \ldots, f(n), f(n+1)\} = F' \cup \{f(n+1)\}$$

où

$$F' = \{f(1), \ldots, f(n)\}.$$

$\mathfrak{P}(n)$ étant vrai, F' a un plus grand élément p; il en résulte que F a un plus grand élément qui est $\sup\{p, f(n+1)\}$; donc si $\mathfrak{P}(n)$ est vrai, il en est de même de $\mathfrak{P}(n+1)$. $\mathfrak{P}(n)$ est donc vrai pour tout n de $\mathbb{N}^*$.

Réciproquement soit F une *partie majorée non vide* de $\mathbb{N}$, elle a un plus grand élément p (cf § 1.3 *b*); donc pour tout x de F on a $0 \leqslant x \leqslant p$ c'est-à-dire $F \subset [0, p]$. D'après le résultat 1 du sous-paragraphe a) ci-dessus, comme $[0, p]$ est fini il en est de même de F.

Concluons :

Théorème.
Toute partie non vide de $\mathbb{N}$ est finie si et seulement si elle est majorée.

Corollaire.
Quel que soit a de $\mathbb{N}$, $[a, +\infty[$ est une partie infinie de $\mathbb{N}$.

Comme $\mathbb{N} = [0, +\infty[$ on voit que $\mathbb{N}$ **est un ensemble infini.**

Application aux parties non vides finies d'un ensemble totalement ordonné.

Le raisonnement par récurrence ci-dessus, démontrant que toute partie non vide finie de $\mathbb{N}$ a un plus grand élément, n'utilise en fait que le résultat suivant : toute partie de $\mathbb{N}$ ayant 1 ou 2 éléments a un plus grand élément. Or toute partie, ayant 1 ou 2 éléments, de tout ensemble totalement ordonné a un plus grand élément. D'où

Théorème.
Toute partie finie non vide d'un ensemble totalement ordonné a un plus grand élément.

On démontrerait de même que toute partie finie non vide d'un ensemble totalement ordonné a un plus petit élément.
Si $F = \{a_1, a_2, \ldots, a_n\}$, ce plus petit élément α et ce plus grand élément β de F se notent respectivement

$$\inf(a_1, \ldots, a_n) \quad \text{et} \quad \sup(a_1, \ldots a_n)$$

car vous verrez sans peine que α est le plus grand des minorants de F et β le plus petit des majorants de F (cf. § 1.2 d).

1.7 SUITES D'ÉLÉMENTS D'UN ENSEMBLE

a) Notation indicielle.

Définition.
On appelle **suite** d'éléments d'un ensemble X toute application d'une partie de $\mathbb{N}$ dans X.

Soit I une partie de $\mathbb{N}$. Considérons l'application

$$\begin{aligned} f : I &\longrightarrow X \\ n &\longmapsto f(n) \end{aligned}$$

On utilise souvent à la place de $f(n)$ la *notation indicielle* x_n.
n entier naturel élément de I est un **indice.**
La suite, application de I dans X, se notera $(x_n)_{n \in I}$; on dit encore que c'est une **suite indexée.**
On ne confondra pas

- $(x_n)_{n \in I}$, *application* f de I dans X.
- x_n élément de X, *valeur* $f(n)$ de f pour n.

La suite $(x_n)_{n\in I}$ est donc définie par l'ensemble des couples (n, x_n) lorsque n décrit I. On dit que x_n est le **terme d'indice n** de la suite $(x_n)_{n\in I}$.
Si I est une *partie finie* (resp. *infinie*) de $\mathbb{N}$ on dit que la suite $(x_n)_{n\in I}$ est une **suite finie** (resp. **infinie**).
Par exemple $(x_n)_{n\in\mathbb{N}}$, $(x_n)_{n\in\mathbb{N}^*}$ sont des suites infinies.
Si $I = [a, b]$ $(a \leqslant b)$ la suite $(x_n)_{n\in I}$ est finie. On la notera $(x_n)_{a\leqslant n\leqslant b}$.
ATTENTION. Une suite finie prend un nombre fini de valeurs.
En revanche il peut arriver que l'*ensemble des valeurs* d'une *suite infinie* soit *fini*. Par exemple la suite définie pour tout p de $\mathbb{N}$ par

$$x_{2p} = a \quad \text{et} \quad x_{2p+1} = b$$

est une suite infinie à *deux* valeurs, en supposant $a \neq b$.
Si $J \subset I \subset \mathbb{N}$, on dit que la suite $(x_n)_{n\in J}$ est une **suite extraite** de la suite $(x_n)_{n\in I}$.
Autrement dit, en tant qu'application, une suite extraite est une restriction.
On dit qu'une suite infinie $(x_n)_{n\in I}$ est **stationnaire** s'il existe un entier naturel p tel que

$$(\forall\, n \in [p, +\infty[\cap I) \quad x_n = x_p.$$

Par exemple si $I = \mathbb{N}$ cela signifie que la suite considérée est constante sur $[p, +\infty[$.

b) Construction d'une suite par récurrence.

Nous allons construire par récurrence une suite $(x_n)_{n\in\mathbb{N}}$ d'éléments d'un ensemble X. Supposons que l'on se donne $x_0 \in X$ et que l'on possède un procédé permettant, en supposant x_n construit, de construire x_{n+1} et ceci pour tout n de $\mathbb{N}$. Si on désigne par $\mathcal{P}$ la propriété *définie* pour n de $\mathbb{N}$ par « on sait construire x_n », on voit que l'on a
1. $\mathcal{P}(0)$.
2. $(\forall\, n \in \mathbb{N})\ \ \mathcal{P}(n) \Longrightarrow \mathcal{P}(n+1)$.
Donc $\mathcal{P}(n)$ est vrai pour tout n de $\mathbb{N}$. On connaît donc la suite $(x_n)_{n\in\mathbb{N}}$. On dit que cette suite a été *construite par récurrence sur* $\mathbb{N}$.
Vous définirez sans peine une suite construite par récurrence sur $[a, +\infty[$ ou sur $[a, b]$.

Exemple 1.

Soit a un élément de E, ensemble muni d'une *addition ;* on définira la suite $(na)_{n\in\mathbb{N}^*}$ d'éléments de E par

$$1\,a = a$$

et $(\forall\, n \in \mathbb{N}^*)\ \ (n+1)\,a = na + a.$

Si (E, +) a un élément neutre ω, on peut définir la suite $(na)_{n\in\mathbb{N}}$ en posant $0a = \omega$. De même si a est un élément de E, ensemble muni d'une *multiplication* la suite $(a^n)_{n\in\mathbb{N}^*}$ est définie par

$$a^1 = a$$

et $(\forall\, n \in \mathbb{N}^*)\ \ a^{n+1} = a^n a.$

Si (E, $\times$) a un élément neutre e, la suite $(a^n)_{n\in\mathbb{N}}$ est définie en partant de $a^0 = e$.

Par exemple, f étant une application de A dans A, la *$n^{\text{ième}}$ itérée de f*, notée f_n, sera définie par

$$f_0 = \mathrm{Id}_A$$

et $(\forall\, n \in \mathbb{N})\ f_{n+1} = f_n \circ f.$

S'il n'y a pas de multiplication définie dans A, la $n^{\text{ième}}$ itérée de f pourra se noter f^n. En revanche s'il y a une multiplication dans A, f^n est l'application de A dans A définie pour tout x de A par $f^n(x) = [f(x)]^n$; dans ce cas, il faut adopter pour la $n^{\text{ième}}$ itérée de f une notation autre que f^n, par exemple f_n.

EXERCICES

On utilise les notations ci-dessus et l'addition et la multiplication dans E sont associatives.

1. Démontrer que, quels que soient les entiers naturels p et q et quel que soit a de E, on a
$$pa + qa = (p + q)\,a \quad , \quad q\,(pa) = (qp)\,a,$$
$$a^p a^q = a^{p+q}, \qquad (a^p)^q = a^{pq},$$
(Prendre p quelconque fixé et raisonner par récurrence sur q.)

2. Démontrer que, quel que soit l'entier naturel n et quels que soient a et b de E, on a
$$n\,(a + b) = na + nb$$
(l'addition dans E étant associative et commutative).
La multiplication dans E étant associative et commutative, on a
$$(ab)^n = a^n b^n$$
(Raisonner par récurrence sur n.)

Exemple 2. Composé d'une suite finie d'éléments de (E, T).

Soit $(a_k)_{1\leqslant k\leqslant n}$ une suite d'éléments de E muni d'une loi interne notée T. Considérons la suite $(c_k)_{1\leqslant k\leqslant n}$ définie par
$$c_1 = a_1$$
et $(\forall\, k \in [1\,,\, n-1])$ $\qquad c_{k+1} = c_k \,\mathsf{T}\, a_{k+1}$,

l'élément c_n de E ainsi construit est par définition, le **composé des éléments de la suite** $(a_k)_{1\leqslant k\leqslant n}$. On peut écrire
$$c_3 = (a_1 \,\mathsf{T}\, a_2) \,\mathsf{T}\, a_3,$$
$$c_4 = ((a_1 \,\mathsf{T}\, a_2) \,\mathsf{T}\, a_3) \,\mathsf{T}\, a_4,$$
$$c_5 = (((a_1 \,\mathsf{T}\, a_2) \,\mathsf{T}\, a_3) \,\mathsf{T}\, a_4) \,\mathsf{T}\, a_5.$$
$$\ldots\ldots$$

Si la loi T est **associative** nous admettrons que c_n n'est pas modifié si l'on remplace deux éléments consécutifs quelconques de la suite (a_k) par leur composé et ceci autant de fois que l'on voudra. On notera alors le composé c_n
$$c_n = a_1 \,\mathsf{T}\, a_2 \,\mathsf{T}\, \ldots \,\mathsf{T}\, a_n = \overset{k=n}{\underset{k=1}{\mathsf{T}}} a_k.$$

Par exemple pour l'addition
$$c_n = a_1 + a_2 + \ldots + a_n = \sum_{k=1}^{k=n} a_k$$

et pour la multiplication
$$c_n = a_1 a_2 \ldots a_n = \prod_{k=1}^{k=n} a_k.$$

Dans ces notations (des derniers membres de ces égalités) k est un *indice muet;* on peut le remplacer par n'importe quelle lettre non utilisée dans la question; on a par exemple, si $m < n$
$$a_m + a_{m+1} + \ldots a_n = \sum_{k=m}^{k=n} a_k = \sum_{i=m}^{i=n} a_i, \quad \text{etc.}$$

En revanche on ne peut utiliser à la place de k ni la lettre m, valeur initiale de l'indice de sommation, ni la lettre n, valeur finale de cet indice.

REMARQUE

Si la loi **n'est pas associative,** il faut s'en tenir à la définition donnée au début $c_1 = a_1$ et, pour tout k de $[1, n-1]$, $c_{k+1} = c_k \top a_{k+1}$.
On peut aussi définir la suite $(c'_h)_{1 \leqslant h \leqslant n}$ de la manière suivante

$$c'_1 = a_n,$$

et $\forall\, h \in [1, n-1] \qquad c'_{h+1} = a_{n-h} \top c'_h.$

On a alors

$$c'_2 = a_{n-1} \top a_n,$$
$$c'_3 = a_{n-2} \top (a_{n-1} \top a_n),$$
$$c'_4 = a_{n-3} \top (a_{n-2} \top (a_{n-1} \top a_n)),$$
$$c'_5 = a_{n-4} \top (a_{n-3} \top (a_{n-2} \top (a_{n-1} \top a_n))),$$
$$\ldots\ldots$$

On dit que c'_n a été obtenu en utilisant une **récurrence descendante** sur $[1, n]$.
Naturellement en général $c'_n \neq c_n$.
On utilise ce procédé (récurrence descendante) pour les *puissances superposées*. Par exemple a, b, c, d étant des entiers naturels $\geqslant 1$ on calcule

$$d \quad , \quad c^d \quad , \quad b^{(c^d)} \quad , \quad a^{(b^{(c^d)})};$$

le premier procédé nous donnerait

$$a \quad , \quad a^b \quad , \quad (a^b)^c = a^{bc} \quad , \quad \left((a^b)^c\right)^d = (a^{bc})^d = a^{bcd}.$$

Exemple 3. Factorielle n.

La suite notée $(n!)_{n \in \mathbb{N}}$ est définie par

$$0! = 1$$

et $(\forall\, n \in \mathbb{N})\ (n+1)! = (n!)\,(n+1).$

On voit que

$$1! = 1 \quad , \quad 2! = 2 \quad , \quad 3! = 6 \quad , \quad 4! = 24 \quad , \quad 5! = 120 \ldots$$

et d'une façon générale pour $n \geqslant 2$

$$n! = 1 \times 2 \times 3 \times \ldots \times n.$$

Le symbole $n!$ se lit « **factorielle n** ».

1.8 APPLICATIONS D'UN ENSEMBLE FINI DANS UN ENSEMBLE FINI

a) Caractérisation des surjections et des bijections.

Soit une application f de E dans F; nous posons

$$\text{card E} = p \geqslant 1 \quad \text{et} \quad \text{card F} = n \geqslant 1.$$

L'image $f(\text{E})$ de E par f est une partie de F; c'est donc un ensemble fini et on a

$$r = \text{card}\, f(\text{E}) \leqslant \text{card F}.$$

Si f est surjective on a $f(\text{E}) = \text{F}$ donc $r = n$.
Si f n'est pas surjective on a $f(\text{E}) \neq \text{F}$ donc $r < n$.
L'ensemble E étant non vide, $r = \text{card}\, f(\text{E}) \geqslant 1$, posons

$$f(\text{E}) = \{y_1, y_2, \ldots, y_r\};$$

les éléments $y_1 \ldots y_r$ sont deux à deux distincts; posons également pour tout i de $[1, r]$

$$\text{E}_i = \{x \in \text{E} \mid f(x) = y_i\}.$$

Les E_i sont des parties de E fini; ce sont donc des ensembles finis. Ces parties sont non vides et d'après la définition de $f(E)$, chaque x de E appartient à un et un seul des éléments de la suite $(E_i)_{1 \leqslant i \leqslant r}$. Donc cette suite définit une *partition* de E; on a donc

$$\text{card } E = \sum_{i=1}^{i=r} \text{card } E_i$$

Comme card $E_i \geqslant 1$ on a

$$\text{card } E \geqslant r.$$

Si l'application f est injective, pour tout i de $[1, r]$ card $E_i = 1$ donc $p = r$; si l'application f n'est pas injective, il existe au moins une partie E_i telle que card $E_i > 1$; dans ce cas on a donc $p > r$.
Concluons :

Théorème.

Pour toute application f de E fini dans F fini on a

$$\text{card } f(E) \leqslant \inf (\text{card E}, \text{card F}).$$

L'application f est surjective si et seulement si card $f(E)$ = card F.
L'application f est injective si et seulement si card $f(E)$ = card E.

Vous démontrerez sans peine le corollaire suivant :

Corollaire.

Si E et F sont deux ensembles **finis** tels que

$$\text{card E} = \text{card F}$$

pour toute application f de E dans F les trois propriétés suivantes sont équivalentes
i. f est bijective,
ii. f est injective,
iii. f est surjective.

EXERCICES

1. Démontrer que la relation $f(x) = f(x')$ définit une relation d'équivalence sur E. Quelles sont les classes d'équivalence pour cette relation?
(On posera $f(E) = \{y_1, \ldots, y_r\}$).
2. Avec les mêmes notations que ci-dessus on suppose que pour tout i de $[1, r]$ card $E_i = h$. Démontrer que card $E = rh$.
3. Soit deux ensembles finis A et B tels que card $A = a \geqslant 1$ et card $B = b \geqslant 1$. En appliquant le résultat de l'exercice 2 à l'application (première projection de $A \times B$ sur A)

$$f : A \times B \longrightarrow A$$
$$(x, y) \longmapsto x$$

démontrer que card $(A \times B) = ab$.

Soit A et B finis; si $A = \varnothing$ ou $B = \varnothing$, alors $A \times B = \varnothing$. Avec le résultat de l'exercice 2 nous pouvons énoncer

Quels que soient les ensembles finis A et B on a

$$\text{card } (A \times B) = (\text{card A}) \cdot (\text{card B}).$$

b) Nombre des applications de E fini dans F fini.

Soit $E_p = \{a_1, a_2, \ldots a_p\}$ un ensemble fini de cardinal $p \geqslant 1$ et $F_n = \{b_1, b_2, \ldots, b_n\}$ un ensemble fini de cardinal $n \geqslant 1$.

Nous nous proposons de montrer que l'ensemble $\mathcal{F}(E_p, F_n)$ des applications de E_p dans F_n est fini et de calculer son cardinal.
Nous supposerons n élément fixé de $\mathbb{N}^*$ et nous ferons une *récurrence* sur q, appartenant à $[1, p]$, q étant le cardinal de l'ensemble de départ.
Si $q = 1$, il y a n applications de E_1 dans F_n; ce sont les applications $f_1, f_2 \ldots f_n$, deux à deux distinctes, définies respectivement par

$$f_1(a_1) = b_1 \quad , \quad f_2(a_1) = b_2 \quad , \quad \ldots \quad , \quad f_n(a_1) = b_n.$$

Donc $\mathcal{F}(E_1, F_n)$ *est fini et on a*

$$\text{card } \mathcal{F}(E_1, F_n) = n.$$

Supposons que, pour q tel que $1 \leqslant q \leqslant p - 1$, l'ensemble $\mathcal{F}(E_q, F_n)$ soit fini (hypothèse de récurrence).
Soit f' un élément quelconque de $\mathcal{F}(E_{q+1}, F_n)$, sa *restriction* à E_q est un élément de $\mathcal{F}(E_q, F_n)$; donc f' est un *prolongement* à E_{q+1} d'un élément f de $\mathcal{F}(E_q, F_n)$.
Cherchons donc tous les prolongements f' à E_{q+1} de f, application de E_q dans F_n, on a

$$\text{(I)} \qquad \begin{cases} (\forall x \in E_q) \quad f'(x) = f(x), \\ f'(a_{q+1}) \in F_n. \end{cases}$$

La valeur $f'(a_{q+1})$ peut être un élément quelconque de F_n. Donc chaque application f de E_q dans F_n donne naissance à n prolongements f', applications de E_{q+1} dans F_n. Ces n prolongements de f sont *distincts :* ils diffèrent par leur valeur pour a_{q+1}. Considérons deux applications f' et g' de E_{q+1} dans F_n, prolongements respectifs de *deux applications distinctes* f et g de E_q dans F_n. Il existe donc $a_i \in E_q$ tel que $f(a_i) \neq g(a_i)$, donc $f'(a_i) \neq g'(a_i)$ et f' et g' sont donc des applications distinctes.
Concluons :
Tout élément de $\mathcal{F}(E_{q+1}, F_n)$ *est un prolongement d'un élément de* $\mathcal{F}(E_q, F_n)$.
Chaque élément de $\mathcal{F}(E_q, F_n)$ *donne naissance à n prolongements à* E_{q+1}, *éléments de* $\mathcal{F}(E_{q+1}, F_n)$.
Tous les prolongements obtenus sont distincts.
Il résulte de ces propriétés que $\mathcal{F}(E_{q+1}, F_n)$ est fini et que l'on a pour tout entier q tel que $1 \leqslant q \leqslant p - 1$:

$$\text{(1)} \qquad \text{card } \mathcal{F}(E_{q+1}, F_n) = n \text{ card } \mathcal{F}(E_q, F_n).$$

L'énoncé « $\mathcal{F}(E_q, F_n)$ est fini pour tout q de $[1, p]$ » est donc vrai; donc $\mathcal{F}(E_p, F_n)$ est fini.
De plus on peut écrire

$$\begin{aligned} &\text{card } \mathcal{F}(E_1, F_n) = n, \\ &\text{card } \mathcal{F}(E_2, F_n) = n \text{ card } \mathcal{F}(E_1, F_n), \\ &\text{card } \mathcal{F}(E_3, F_n) = n \text{ card } \mathcal{F}(E_2, F_n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\text{card } \mathcal{F}(E_p, F_n) = n \text{ card } \mathcal{F}(E_{p-1}, F_n), \end{aligned}$$

en multipliant membre à membre ces p égalités et en simplifiant on obtient :

$$\text{(2)} \qquad \boxed{\text{card } \mathcal{F}(E_p, F_n) = n^p}. \qquad (p \in \mathbb{N}^*, n \in \mathbb{N}^*)$$

Théorème.
Le nombre des applications d'un ensemble à $p \geqslant 1$ éléments dans un ensemble à $n \geqslant 1$ éléments est n^p.

c) Nombre des injections de E fini dans F fini.

Prenons les mêmes notations que ci-dessus. S'il existe au moins une *injection* de E_p dans E_n on a $p \leqslant n$. Nous supposerons donc card $E_p = p$, card $E_n = n$ avec $1 \leqslant p \leqslant n$.
Désignons par $\mathfrak{I}(E_p, F_n)$ l'ensemble des injections de E_p dans F_n.
Ici il est inutile de démontrer que $\mathfrak{I}(E_p, F_n)$ est fini, car cet ensemble est une partie de l'ensemble fini $\mathcal{F}(E_p, F_n)$.
Si $p = 1$, il y a n applications de E_1 dans F_n et ce sont toutes des injections, donc

$$\text{card } \mathfrak{I}(E_1, F_n) = n.$$

Supposons connu card $\mathfrak{I}(E_q, F_n)$ pour $1 \leqslant q \leqslant p-1$ et calculons card $\mathfrak{I}(E_{q+1}, F_n)$.
Soit i' un élément quelconque de $\mathfrak{I}(E_{q+1}, F_n)$, *sa restriction* à E_q est une *injection* de E_q dans F_n, c'est-à-dire un élément de $\mathfrak{I}(E_q, F_n)$, dont i' est un *prolongement injectif* à E_{q+1} de i élément de $\mathfrak{I}(E_q, F_n)$.
Cherchons donc tous les prolongements injectifs i' à E_{q+1} d'un élément i de $\mathfrak{I}(E_q, F_n)$; on a

$$\text{(II)} \qquad \begin{cases} (\forall\, x \in E_q)\ \ i'(x) = i(x), \\ i'(a_{q+1}) \in F_n - i(E_q). \end{cases}$$

En effet i' étant un *prolongement injectif* de i la valeur $i'(a_{q+1})$ est un élément de F_n *distinct* de $i'(a_1) = i(a_1)$, $i'(a_2) = i(a_2)$, ..., $i'(a_q) = i(a_q)$. On notera la différence entre la condition (II) ci-dessus et la condition (I) du § 1.8 b.
Donc chaque injection i de E_q dans F_n donne naissance à $n - q$ *prolongements injectifs* de i, injections de E_q dans F_n; car i' étant injective et $i(E_q)$ étant une partie de F_n on a

$$\text{card } i(E_q) = q \quad \text{et} \quad \text{card}\,(F_n - i(E_q)) = n - q.$$

Ces $n - q$ prolongements injectifs de i sont *distincts :* ils diffèrent par leur valeur pour a_{q+1}. Vous verrez sans peine que deux injections i' et j' de E_{q+1} dans F_n, prolongements respectifs de deux *injections distinctes* i et j de E_q dans F_n, sont distinctes.
On conclut que pour tout entier q tel que $1 \leqslant q \leqslant p-1$ on a

$$\text{card } \mathfrak{I}(E_{q+1}, F_n) = (n - q)\ \text{card } \mathfrak{I}(E_q, F_n).$$

On peut donc écrire les égalités :

$$\begin{aligned} &\text{card } \mathfrak{I}(E_1, F_n) = n, \\ &\text{card } \mathfrak{I}(E_2, F_n) = (n-1)\ \text{card } \mathfrak{I}(E_1, F_n), \\ &\text{card } \mathfrak{I}(E_3, F_n) = (n-2)\ \text{card } \mathfrak{I}(E_2, F_n), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\text{card } \mathfrak{I}(E_p, F_n) = [n - (p-1)]\ \text{card } \mathfrak{I}(E_{p-1}, F_n); \end{aligned}$$

en multipliant membre à membre ces p égalités et en simplifiant on obtient :

$$\boxed{\text{card } \mathfrak{I}(E_p, F_n) = n(n-1)(n-2)\ldots(n-p+1)} \qquad (1 \leqslant p \leqslant n).$$

Théorème.

Le nombre des injections d'un ensemble ayant p éléments dans un ensemble ayant n éléments $(1 \leqslant p \leqslant n)$ est

$$n(n-1)\ldots(n-p+1).$$

Ce nombre peut aussi s'écrire

$$\frac{n(n-1)\ldots(n-p+1)\,[(n-p)(n-p-1)\ldots\times 2\times 1]}{(n-p)(n-p-1)\ldots\times 2\times 1} = \frac{n!}{(n-p)!}$$

Si card E = card F = n, nous avons vu au § 1.8 a que f, application de E dans F est *bijective* si et seulement si f est injective; or le nombre des injections de E dans F est, si $n = p$, $\frac{n!}{0!} = n!$ d'où

Corollaire.

Le nombre des bijections d'un ensemble à n éléments sur un ensemble à n éléments est $n!$

En particulier si card E = n, le nombre des *permutations* de E, c'est-à-dire des bijections de E sur lui-même est $n!$

d) Nombre de parties ayant p éléments d'un ensemble fini.

Soit E un ensemble fini non vide ayant n éléments ($n > 0$). Désignons par $\mathfrak{T}_p$ (E) l'ensemble des parties de E ayant p éléments ($p \leqslant n$); cherchons card $\mathfrak{T}_p$ (E).
Pour $p = 0$, il y a une seule partie, la partie vide $\varnothing$.
Supposons $p > 0$ et désignons par P l'ensemble

$$P = [1\ ,\ p] = \{1, 2, \ldots, p\}.$$

Si i est une injection de P dans E, i (P) est une partie de E ayant p éléments (cf. § 1.8 a). Toute partie $A \in \mathfrak{T}_p$ (E) peut être obtenue comme image d'une injection i de P dans E, mais de plusieurs manières; A, élément de $\mathfrak{T}_p$ (E), étant donné, cherchons le nombre d'injections i de P dans E telles que

$$i\,(P) = A.$$

A chacune de ces injections i est associée une bijection unique b de P sur A telle que pour tout x de P on ait $b\,(x) = i\,(x)$. *Il existe donc autant d'injections de* P *dans* E *telles que* i (P) = A *que de bijections de* P *sur* A, c'est-à-dire $p!$. Par conséquent A est l'image de P par $p!$ injections distinctes, on a donc

$$\text{card } \mathfrak{I}\,(P, E) = p!\ \text{card } \mathfrak{T}_p\,(E)$$

d'où

$$\text{card } \mathfrak{T}_p\,(E) = \frac{n\,(n-1)\ldots(n-p+1)}{p!} = \frac{n!}{p!\,(n-p)!}.$$

Remarquons que la formule s'applique pour $p = 0$, on retrouve $\frac{n!}{0!\,n!} = 1$. Cette formule s'applique même pour $n = p = 0$: l'ensemble vide admet lui-même pour seule partie. Ce nombre est représenté par le symbole C_n^p ou encore par $\binom{n}{p}$ (notez la place des indices n et p dans les deux symboles).

Théorème.

Le nombre des parties à p éléments d'un ensemble à n éléments ($0 \leqslant p \leqslant n$) est

$$\boxed{C_n^p = \frac{n!}{p!\,(n-p)!}}.$$

Les entiers naturels C_n^p ($0 \leqslant p \leqslant n$) interviennent dans la *formule du binôme* (cf. § 3.10 b); ils sont appelés **coefficients binomiaux.**

EXERCICES

4. Démontrer que, quels que soient les entiers naturels n et p vérifiant $0 \leqslant p \leqslant n$, on a $C_n^p = C_n^{n-p}$. Interpréter cette formule en associant à chaque partie A de E son complémentaire dans E.

5. Démontrer que, quels que soient les entiers naturels n et p vérifiant $1 \leqslant p \leqslant n$, on a

$$C_n^p = C_{n-1}^{p-1} + C_{n-1}^p.$$

Interpréter cette formule en distinguant un élément a de E et en comptant les parties à p éléments de E contenant a et les parties à p éléments de E ne contenant pas a.

6. Dresser le tableau des C_n^p pour $1 \leqslant n \leqslant 7$ (Triangle de PASCAL).

II. Division euclidienne dans $\mathbb{N}$ Systèmes de numération

1.9 DIVISION EUCLIDIENNE DANS $\mathbb{N}$

a) Propriété d'Archimède.

Soit a un élément quelconque de $\mathbb{N}$ et b un élément quelconque de $\mathbb{N}^*$ on a

$$(a + 1)\, b = ab + b.$$

Comme $b > 0$ on a $b \geqslant 1$ et par conséquent $(a + 1)\, b > ab \geqslant a$. Il existe donc $k \in \mathbb{N}$ tel que $a < kb$; concluons :

Lemme d'Archimède.

Quels que soient l'entier naturel a et l'entier naturel $b > 0$ il existe un entier naturel k tel que

$$a < kb.$$

b) Division euclidienne dans $\mathbb{N}$.

Avec les mêmes notations que ci-dessus considérons l'ensemble E des entiers naturels p tels que $a < pb$; d'après le lemme d'Archimède, E est une *partie non vide* de $\mathbb{N}$. Cet ensemble E admet donc un plus petit élément (cf. § 1.3 b). Celui-ci n'est pas nul, puisque $0.b = 0 \leqslant a$. On peut donc représenter ce plus petit élément par $q + 1$ ($q \in \mathbb{N}$), et l'on a $a < (q + 1)\, b$. L'entier naturel $q + 1$ étant le plus petit élément de E, l'entier naturel q n'appartient pas à E; donc $a < qb$ est faux et par suite on a $qb \leqslant a$.
On a donc mis en évidence un *entier naturel unique* q tel que :

$$bq \leqslant a < b\,(q + 1). \qquad (1)$$

Posons : $a - bq = r.$

Des inégalités (1), il résulte que :

$$a - bq \geqslant 0 \quad , \quad \text{soit} \quad r \geqslant 0$$

et

$$a - bq < b \quad , \quad \text{soit} \quad r < b.$$

Concluons :

Théorème et définition.

Quels que soient a de $\mathbb{N}$ de b de $\mathbb{N}^*$ il existe un couple unique (q, r) d'entiers naturels q et r tels que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

L'opération permettant de passer du couple (a, b) au couple (q, r) s'appelle **division euclidienne** de a par b. Les nombres q et r sont respectivement le **quotient** et le **reste** dans cette division.

EXEMPLES

1. $a = 293$, $b = 45$

$$293 = (45 \times 6) + 23,$$

donc $q = 6$ et $r = 23$.

2. $a = 420$, $b = 35$.

$$420 = 35 \times 12$$

donc $q = 12$ et $r = 0$.

Dans ce cas, on dit que 35 divise 420.

3. $a = 75$, $b = 120$.

$$75 = (120 \times 0) + 75,$$

donc $q = 0$ et $r = 75$.

1.10 PRINCIPE DES SYSTÈMES DE NUMÉRATION

Il n'a été question, jusqu'à présent que d'entiers naturels sans que l'on indique de quelle manière les représenter.

Nous nous proposons, dans ce paragraphe, d'étudier la représentation des nombres entiers naturels, à l'aide d'un nombre fini de symboles appelés « chiffres » (comme on écrit des mots avec des lettres).

a) Écriture d'un nombre dans le système de numération de base x. Existence.

La méthode la plus couramment employée est celle qui utilise x symboles

$$\{0, 1, 2, \ldots, (x - 1)\}$$

et qu'on appelle **système de numération de base x, où x est un entier naturel strictement supérieur à 1.**

Remarquons que nous avons indiqué les symboles 0, 1, 2, ... ; ce sont les symboles appelés « *chiffres arabes* ». On pourrait tout aussi bien employer d'autres symboles ($\bigstar$, S, K, $\times$, ...).

Les symboles choisis représentent les x premiers entiers naturels écrits dans l'ordre croissant :

$$0 < 1 < 2 < 3 < \ldots < x - 1.$$

Soit N un nombre entier naturel.

- Si $N < x$, il est représentable par l'un des symboles choisis.
- Si $N \geqslant x$, on peut effectuer la division euclidienne de N par x. On obtient :

$$N = q_1 x + r_0 \quad , \quad 0 \leqslant r_0 < x, \quad q_1 \neq 0.$$

L'entier r_0 est donc représentable par l'un des symboles.

Si $q_1 < x$, il existe également un symbole pour la représenter et on écrira, par convention :

$$N = q_1 x + r_0 = \overline{q_1 r_0}.$$

(Le trait au-dessus de $q_1 r_0$ étant mis pour éviter une confusion avec le produit $q_1 r_0$.)

Par exemple, dans le système de numération de *base dix*, si $N = \overline{23}$, cela signifie $N = 2x + 3$ où x vaut *dix*.
Dans le système de numération de *base cinq*, les symboles sont : 0, 1, 2, 3, 4, et le nombre qui s'écrit $\overline{32}$ est le nombre $N = 3x + 2$ où x vaut *cinq*.

Si $q_1 \geqslant x$, on divise à nouveau q_1 par x, et ainsi de suite jusqu'à ce que l'on obtienne un quotient q_n *inférieur strictement à* x. On obtient ainsi, de façon générale :

$$\begin{array}{l|l} & N = q_1 x + r_0 \quad , \quad 0 \leqslant r_0 < x \quad , \quad q_1 \neq 0 \\ x & q_1 = q_2 x + r_1 \quad , \quad 0 \leqslant r_1 < x \quad , \quad q_2 \neq 0 \\ x^2 & q_2 = q_3 x + r_2 \quad , \quad 0 \leqslant r_2 < x \quad , \quad q_3 \neq 0 \\ \ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x^{n-1} & q_{n-1} = q_n x + r_{n-1}, \quad 0 \leqslant r_{n-1} < x \quad , \quad q_n \neq 0. \end{array}$$

Supposons, par exemple, que q_n soit le premier quotient tel que $q_n < x$ ($n \in \mathbb{N}^*$).
Multiplions chacune des égalités précédentes par un nombre entier convenablement choisi, de telle sorte qu'en ajoutant les égalités obtenues, les q_i ($1 \leqslant i \leqslant n-1$) se trouvent éliminés. Ces nombres sont indiqués en rouge à gauche de chaque égalité. On obtient ainsi :

$$N = q_n x^n + r_{n-1} x^{n-1} + \ldots + r_2 x^2 + r_1 x + r_0,$$

qu'on écrira, par convention :

$$N = \overline{q_n r_{n-1} \ldots r_2 r_1 r_0}$$

puisque chacun des nombres $r_0, r_1, \ldots, r_{n-1}, q_n$, étant strictement inférieur à x, est représentable par l'un des symboles choisis.

EXEMPLE

Soit dans le système de numération de base deux, où les symboles sont 0, 1, le nombre

$$N = 10\,111\,011$$

On a

$$\begin{aligned} N &= 1.x^7 + 1.x^5 + 1.x^4 + 1.x^3 + 1.x + 1 \\ &= x^7 + x^5 + x^4 + x^3 + x + 1 \end{aligned}$$

où x vaut « deux ».

Puisque chacun des nombres $r_0, r_1, \ldots, r_{n-1}, q_n$ est strictement inférieur à x, chacun d'eux est inférieur ou égal à $(x-1)$. Par suite :

$$\begin{array}{ll} & N \leqslant (x-1)x^n + (x-1)x^{n-1} + \ldots + (x-1)x + (x-1), \\ \text{soit :} & N \leqslant (x-1)(x^n + x^{n-1} + \ldots + x + 1), \\ \text{ou encore :} & N \leqslant x^{n+1} - 1, \\ \text{c'est-à-dire :} & N < x^{n+1}. \end{array}$$

b) Unicité de l'écriture d'un nombre dans le système de base x.

Soit une autre représentation :

$$N = \overline{\alpha_p \alpha_{p-1} \ldots \alpha_1 \alpha_0} = \alpha_p x^p + \alpha_{p-1} x^{p-1} + \ldots + \alpha_1 x + \alpha_0,$$

les nombres $\alpha_0, \alpha_1, \ldots, \alpha_p$ étant strictement inférieurs à x et $\alpha_p \neq 0$.
Le nombre $N = (\alpha_p x^{p-1} + \alpha_{p-1} x^{p-2} + \ldots + \alpha_1)x + \alpha_0$ est de la forme $qx + \alpha_0$ avec $\alpha_0 < x$, donc q et α_0 sont *encore* le quotient et le reste *uniques* de la division euclidienne de N par x donc $\alpha_0 = r_0$ et $q = q_1$ avec :

$$\begin{aligned} q &= \alpha_p x^{p-1} + \alpha_{p-1} x^{p-2} + \ldots + \alpha_1 = \overline{\alpha_p \alpha_{p-1} \ldots \alpha_1} \\ q_1 &= q_n x^{n-1} + r_{n-1} x^{n-2} + \ldots + r_1 = \overline{q_n r_{n-1} \ldots r_1}, \end{aligned}$$

on verra de même que $\alpha_1 = r_1$ et ainsi de suite. Si $p > n$ nous aurons $\alpha_0 = r_0$, $\alpha_1 = r_1$, ..., $\alpha_n = q_n$ d'où $\alpha_p x^p + \alpha_{p-1} x^{p-1} + ... + \alpha_{n+1} x^{n+1} = 0$ ce qui n'est possible dans $\mathbb{N}$ que si $\alpha_p = \alpha_{p-1} = ... = \alpha_{n+1} = 0$. On verra de même qu'on ne peut avoir $p < n$. Donc $p = n$. On peut énoncer :

Théorème.

Tout nombre entier naturel N admet une représentation unique dans le système de numération de base x.

En particulier, *quelle que soit la base x*, on a :

$$x = 1.x + 0 = \overline{10}.$$

Par suite, quelle que soit la base x:

$$\begin{aligned} N &= \overline{q_n r_{n-1} r_{n-2} \dots r_2 r_1 r_0} \\ &= q_n \overline{10}^n + r_{n-1} \overline{10}^{n-1} + \dots + r_2 \overline{10}^2 + r_1 \overline{10} + r_0. \end{aligned}$$

N peut s'écrire :

$$\begin{aligned} N &= (q_n x^n + r_{n-1} x^{n-1} + \dots + r_p x^p) + (r_{p-1} x^{p-1} + \dots + r_2 x^2 + r_1 x + r_0) \\ &= (q_n x^{n-p} + r_{n-1} x^{n-p-1} + \dots + r_p) x^p + R, \end{aligned}$$

avec $$R = \overline{r_{p-1} r_{p-2} \dots r_2 r_1 r_0}.$$

D'après ce qui précède : $0 \leqslant R < x^p$, et par suite R représente le reste de la division euclidienne de N par x^p, le quotient étant $Q = q_n x^{n-p} + r_{n-1} x^{n-p-1} + \dots + r_p$; soit :

$$Q = \overline{q_n r_{n-1} \dots r_p} \quad \text{et} \quad R = \overline{r_{p-1} \dots r_2 r_1 r_0}.$$

Corollaire.

Le reste de la division par x^p d'un nombre N écrit dans le système de numération de base x est égal au nombre formé par les p chiffres de droite du nombre N écrit dans cette base.

1.11 COMPARAISON DE NOMBRES ÉCRITS DANS LE SYSTÈME DE NUMÉRATION DE BASE x

a) Comparaison d'un nombre aux puissances de la base.

Considérons le nombre $N = \overline{q_n r_{n-1} \dots r_2 r_1 r_0}$, où $q_n \neq 0$. Nous avons vu que l'on a

$$N < x^{n+1}.$$

D'autre part on a :

$$N = q_n x^n + A \quad \text{avec} \quad A = r_{n-1} x^{n+1} + \dots + r_1 x + r_0,$$

et $$0 < q_n < x, \quad \text{d'où} \quad q_n \geqslant 1.$$

On en déduit que $N \geqslant x^n$. Concluons :

Quel que soit l'entier naturel écrit dans le système de base x :

$$N = \overline{q_n r_{n-1} \dots r_1 r_0}$$

avec $q_n \neq 0$, on a :

$$x^n \leqslant N < x^{n+1}.$$

b) Comparaison de deux nombres quelconques écrits dans la base x.

Premier cas : Les deux nombres N et N′ ne sont pas écrits avec le même nombre de chiffres.

$N = \overline{q_n r_{n-1} \dots r_2 r_1 r_0}$. Il a $(n+1)$ chiffres avec $q_n \neq 0$.
$N' = \overline{q'_{n'} r'_{n'-1} \dots r'_2 r'_1 r'_0}$. Il a $(n'+1)$ chiffres avec $q'_{n'} \neq 0$.
D'après le résultat ci-dessus :

$$x^n \leqslant N < x^{n+1}$$
$$x^{n'} \leqslant N' < x^{n'+1}$$

Supposons $n < n'$; alors $n+1 \leqslant n'$, et par suite :

$$x^n \leqslant N < x^{n+1} \leqslant x^{n'} \leqslant N' < x^{n'+1}.$$

On en déduit que $N < N'$. Concluons :

Si deux nombres N et N′ écrits dans le système de numération de base x n'ont pas le même nombre de chiffres, celui qui s'écrit avec le plus de chiffres est le plus grand.

REMARQUE

Si l'on veut représenter une famille d'entiers par le même nombre de chiffres on convient que l'écriture d'un certain nombre de zéros à gauche de l'écriture du nombre ne modifie pas la valeur du nombre représenté. Par exemple en base dix pour les numéros des départements on fait cette convention : le département des Hautes-Alpes est représenté par 05 et non par 5.
Il va sans dire que, dans l'étude précédente, on ne fait pas cette convention : le chiffre le plus à gauche q_n est non nul c'est-à-dire $q_n \geqslant 1$.

Deuxième cas : Les deux nombres N et N′ sont écrits avec le même nombre de chiffres.
$N = \overline{q_n r_{n-1} \dots r_2 r_1 r_0}$. Il a $(n+1)$ chiffres avec $q_n \neq 0$.
$N' = \overline{q'_n r'_{n-1} \dots r'_2 r'_1 r'_0}$. Il a aussi $(n+1)$ chiffres avec $q'_n \neq 0$.
• *Supposons* $q_n < q'_n$.
D'après le corollaire du § 1.10 b

$$R = \overline{r_{n-1} \dots r_1 r_0} \quad \text{et} \quad R' = \overline{r'_{n-1} \dots r'_1 r'_0}$$

sont les restes des divisions euclidiennes de N et N′ par x^n et l'on a

$$N = q_n x^n + R \quad , \quad 0 \leqslant R < x^n,$$
et $$N' = q'_n x^n + R' \quad , \quad 0 \leqslant R' < x^p.$$

Par suite :

$$q_n x^n \leqslant N < (q_n + 1) x^n,$$
et $$q'_n x^n \leqslant N' < (q'_n + 1) x^n.$$

Puisque l'on a supposé $q_n < q'_n$, c'est-à-dire

$$q_n + 1 \leqslant q'_n,$$

on en déduit :

$$q_n x^n \leqslant N < (q_n + 1) x^n \leqslant q'_n x^n \leqslant N' < (q'_n + 1) x^n,$$

et, par suite : $$N < N'.$$

• *Supposons* $q_n = q'_n$ et de plus qu'il existe un rang p tel que :
$r_p < r'_p$ et, pour tout indice k vérifiant $p < k < n$, $r_k = r'_k$.
On a alors :

$$N - \overline{(q_n r_{n-1} \dots r_{p+1})} x^{p+1} = \overline{r_p r_{p-1} \dots r_2 r_1 r_0} = R,$$
et : $$N' - \overline{(q_n r_{n-1} \dots r_{p+1})} x^{p+1} = \overline{r'_p r'_{p-1} \dots r'_2 r'_1 r'_0} = R'.$$

Les deux nombres R et R′ ont le même nombre de chiffres et $r_p < r'_p$, donc $R < R'$ et par suite $N < N'$.
Concluons :

> Si deux nombres N et N′ écrits dans le système de numération de base x ont le même nombre de chiffres, la comparaison de leurs chiffres distincts de même rang le plus grand possible permet de les comparer, et ils sont dans le même ordre que ces deux chiffres.

1.12 EXEMPLES DE CALCULS DANS LE SYSTÈME DE NUMÉRATION DE BASE DEUX

a) Addition de deux nombres.

La table d'addition dans le système de « base deux » est la suivante :

a / b	0	1
0	0	1
1	1	10

On remarque en effet que, x valant « deux », on a

$$1 + 1 = x = (1 \times x) + 0 = 10.$$

Effectuons :

$$\begin{array}{r} {\scriptstyle 1\ 11} \\ 1\,011\,001 \\ +\quad 101\,101 \\ \hline 10\,000\,110 \end{array}$$

Chaque « retenue » est indiquée en rouge.
(Nous n'avons pas surligné les nombres puisqu'il n'y a aucune confusion possible.)

b) Multiplication de deux nombres.

1. *Multiplication par* $\overline{10}^k$ (démonstration valable pour une base x quelconque).

Si $N = \overline{q_n r_{n-1} \dots r_1 r_0}$

$= q_n \times \overline{10}^n + r_{n-1} \times \overline{10}^{n-1} + \dots + r_1 \times \overline{10} + r_0,$

alors $N \times \overline{10}^k = q_n \times \overline{10}^{n+k} + r_{n-1} \times \overline{10}^{n+k-1} + \dots + r_1 \overline{10}^{k+1} + r_0 \times \overline{10}^k$

et par suite :

$N \times \overline{10}^k = \overline{q_n r_{n-1} \dots r_1 r_0 \underbrace{00 \dots 0}_{k \text{ zéros}}}$

> Pour multiplier un nombre par 10^k, il suffit de juxtaposer k zéros à droite du nombre.

2. Soit à multiplier $N = 1101$ par $N' = 11011$.

Remarquons que la distributivité de la multiplication par rapport à l'addition dans $\mathbb{N}$ nous permet d'écrire (nous ne surlignons pas, il s'agit uniquement de nombres écrits en base deux) :

$$\begin{aligned} N \times N' &= 1101 \times 11011 = 1101 \times (1 + 10 + 10^3 + 10^4) \\ &= 1101 + (1101 \times 10) + (1101 \times 10^3) + (1101 \times 10^4) \\ &= 1101 + 11010 + 1101000 + 11010000, \end{aligned}$$

que nous disposons pratiquement de la façon suivante :

$$\begin{array}{r} 1101 \\ \times\ 11011 \\ \hline 1101 \\ 1101. \\ 1101... \\ 1101.... \\ \hline 101011111 \end{array}$$

où chaque point représente les zéros que l'on juxtapose à la fin du nombre N lors des multiplications de N par les puissances de 10.

EXERCICES

Exercices de révision sur les relations et les applications : ex. 1 à 10, 16, 64.

Calculs dans $\mathbb{N}$: ex. 11 à 14, 16, 17.

Raisonnement par récurrence : ex. 18 à 25, 31, 33.

Suites : ex. 26 à 28, 63.

Problèmes de dénombrement. Coefficients binomiaux : ex. 29 à 37, 65.

Systèmes de numération : ex. 38 à 62.

1.1 On considère les deux applications f et g de $\mathbb{N}$ dans $\mathbb{N}$ définies pour tout n de $\mathbb{N}$ par $f(n) = 2n$ et $g(n) = \frac{n}{2}$ si n est pair et $g(n) = 0$ si n est impair.

a) Étudier l'injectivité et la surjectivité de f et de g.

b) Déterminer $g \circ f$ et $f \circ g$.

1.2 On considère deux applications f de E dans F et g de F dans E telles que $g \circ f = \mathrm{Id}_E$.

a) Démontrer que f est injective et que g est surjective.

b) On suppose de plus E et F *finis* et ayant le même cardinal. Démontrer que f est bijective et que $g = f^{-1}$. (L'exercice 1.1 montre que ce résultat peut être faux si E et F sont infinis, même si E et F sont équipotents).

1.3 On considère deux applications f de E dans F et g de F dans G.

a) Démontrer que si $g \circ f$ est injective, alors f est injective.

b) Démontrer que si $g \circ f$ est surjective, alors g est surjective. (L'exercice 1.2 *a* donne un cas particulier de ces situations).

1.4 Soit f une application de E dans F.

a) Démontrer que la relation $f(x) = f(x')$ est une relation d'équivalence $\mathcal{R}$ dans E.

b) Soit $\dot{x}$ la classe de x, modulo $\mathcal{R}$. Démontrer que l'application φ de E/$\mathcal{R}$ dans f(E) définie pour tout x de E par $\varphi(\dot{x}) = f(x)$ est une bijection.

c) Étudier les exemples suivants :

1. $E = F = \mathbb{R}$ $\quad f(x) = x^2$.
2. $E = F = \mathbb{R}$ $\quad f(x) = \sin x$.

1.5* Soient deux relations binaires $\mathcal{R}_1$ et $\mathcal{R}_2$ dans E, de graphes respectifs R_1 et R_2. Quel que soit (x, y) de E × E on pose

$$\mathcal{R}(x, y) \iff (\mathcal{R}_1(x, y) \text{ et } \mathcal{R}_2(x\, y))$$
$$\mathcal{R}'(x, y) \iff (\mathcal{R}_1(x, y) \text{ ou } \mathcal{R}_2(x, y))$$

a) Quels sont les graphes R et R′ des relations $\mathcal{R}$ et $\mathcal{R}'$?

b) On suppose que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des relations d'équivalence.
Démontrer que $\mathcal{R}$ est une relation d'équivalence. En est-il de même de $\mathcal{R}'$?
Démontrer que toute classe modulo $\mathcal{R}$ est l'intersection d'une classe modulo $\mathcal{R}_1$ et d'une classe modulo $\mathcal{R}_2$.

c) On suppose que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des relations d'ordre.
Démontrer que $\mathcal{R}$ est une relation d'ordre. En est-il de même de $\mathcal{R}'$?
On suppose que $\mathcal{R}_1$ et $\mathcal{R}_2$ sont des relations d'ordre total distinctes; l'ordre défini par $\mathcal{R}$ est-il total?

1.6 Soit a un entier naturel. Démontrer que la relation $\mathcal{R}$ dans $\mathbb{N}$ définie, pour tout (x, y) de $\mathbb{N} \times \mathbb{N}$, par « $x + y = a$ ou $x = y$ » est une relation d'équivalence. Quelles sont les classes d'équivalence?

1.7 On définit dans $\mathbb{N} \times \mathbb{N}$ la relation $\mathcal{R}$ entre (a, a') et (b, b') par « $a \leqslant b$ et $a' \leqslant b'$ ».

a) Démontrer que $\mathcal{R}$ est une relation d'ordre; on la notera $(a, a') \leqslant (b, b')$. Cet ordre est-il total?

b) On considère A = {(1, 2), (2, 3), (3, 1), (3, 2), (3, 4), (4, 3), (4, 4), (5, 5)}.
Indiquez des minorants de A, des majorants de A.
La partie A a-t-elle un plus grand élément? un plus petit élément?

1.8 Soit E muni d'une relation d'ordre $\mathcal{R}$. On dit que a est un élément *minimal* (resp. *maximal*) de A, partie de E, s'il n'y a pas dans A d'élément strictement plus petit (resp. grand) que a.

a) Soit X un ensemble, on pose $\mathcal{T}(X) = E$, la relation est l'inclusion. E a-t-il des éléments maximaux? minimaux? combien?
Soit A l'ensemble des parties propres de E; déterminer les éléments minimaux et les éléments maximaux de A.

b) On prend les notations de l'exercice 1.7. Déterminer les éléments maximaux et les éléments minimaux de A.

1.9 *a*) Démontrer que dans $\mathbb{N}^*$ la relation « x est un multiple de y » est une relation d'ordre; on la notera $x \preccurlyeq y$.

b) Y a-t-il dans $\mathbb{N}^*$ des éléments maximaux? minimaux? (cf. ex. 1.8).

c) Même question dans $\mathbb{N}^* - \{1\}$.

1.10* Soit $\mathcal{T}$ une relation réflexive et transitive définie dans E. On considère la relation $\mathcal{R}$ définie pour tout (x, y) de $E \times E$ par :

$$\mathcal{R}(x, y) \Longleftrightarrow (\mathcal{T}(x, y) \quad \text{et} \quad \mathcal{T}(y, x))$$

a) Démontrer que $\mathcal{R}$ est une relation d'équivalence; on la notera $\equiv$.

b) Démontrer que quels que soient x, x', y, y' de E on a :

$$(\mathcal{T}(x, y) \quad \text{et} \quad x \equiv x' \quad \text{et} \quad y \equiv y') \Longrightarrow \mathcal{T}(x', y').$$

En déduire que l'on peut définir sur $E/\mathcal{R}$ la relation $\mathcal{T}'$, définie pour tout couple $\dot{x}, \dot{y}$ de classes modulo $\mathcal{R}$ par :

$$\mathcal{T}'(\dot{x}, \dot{y}) \Longleftrightarrow \mathcal{T}(x, y).$$

c) Démontrer que $\mathcal{T}'$ est une relation d'ordre.

1.11 Pour tout entier $n \geqslant 1$ et tout entier $p \geqslant 1$ on pose :

$$s_{n,p} = 1^p + 2^p + \ldots + n^p.$$

a) Développer $(1 + k)^2$. Ajouter membre à membre les relations obtenues pour $1 \leqslant k \leqslant n$. En déduire $s_{n,1}$.

b) Procéder de même pour calculer $s_{n,2}$ et $s_{n,3}$ en utilisant respectivement $(1 + k)^3$ et $(1 + k)^4$. (Si l'on connaît la formule du binôme, le même procédé permet de calculer $s_{n,p}$ en fonction de $s_{n,p-1}, \ldots s_{n,2}$ et $s_{n,1}$ en utilisant $(1 + k)^{p+1}$).

En utilisant $s_{n,1}$, $s_{n,2}$, $s_{n,3}$ *(cf. ex. 1.11) calculer les nombres suivants en fonction de* n (ex. 12 à 14).

1.12 $a = 1.2 + 2.3 + \ldots + n(n + 1)$
(On écrira $k(k + 1) = k^2 + k$).

1.13 $b = 1.3.5 + 2.4.6 + \ldots + n(n + 2)(n + 4)$.

1.14 $c = \sum_{k=1}^{k=n} k(n - k + 1)$.

1.15 Démontrer par récurrence (sans utiliser la formule du binôme) que, quels que soient les entiers naturels a et n; on a $(1 + a)^n \geqslant 1 + na$.

1.16 Soit a un entier naturel tel que $a \geqslant 2$. Démontrer que l'application de $\mathbb{N}$ dans $\mathbb{N}$ définie par $n \longmapsto a^n$ est strictement croissante.
En déduire que $a^n = 1$ si et seulement si $n = 0$.

1.17 Soit m, n, p des entiers naturels non nuls.

a) Démontrer que si $n > 2$ et $p > 1$ l'égalité $n^{p-1} = p$ est fausse. Démontrer que pour $n = 2$ l'égalité précédente est vraie seulement pour $p = 1$ ou 2. (Utiliser l'exercice (1.15.)

b) Démontrer que l'égalité :

$$(m^n)^p = m^{(n^p)}$$

est vraie uniquement pour les triplets $(1, n, p)$ $(m, n, 1)$ et $(m, 2, 2)$. (Utiliser l'exercice 1.16.)

Démontrer par récurrence les résultats suivants (cf. ex. 1.11) (ex. 18 à 20).

1.18 $S_{n,1} = \dfrac{n(n+1)}{2}$.

1.19 $S_{n,2} = \dfrac{n(n+1)(2n+1)}{6}$.

1.20 $S_{n,3} = \dfrac{n^2(n+1)^2}{4}$.

1.21 Sachant seulement que $s_{n,1} = \dfrac{n(n+1)}{2}$, démontrer par récurrence que $s_{n,3} = (s_{n,1})^2$.

Démontrer par récurrence les résultats suivants (ex. 22 à 25).

1.22 Quel que soit n de $\mathbb{N}$, $3^{2n} - 2^n$ est divisible par 7.

1.23 Quel que soit n de $\mathbb{N}$, $3^{2n+1} + 2^{n+2}$ est divisible par 7.

1.24 Quel que soit n de $\mathbb{N}^*$, $3^{2n} + 2^{6n-5}$ est divisible par 11.

1.25 Quel que soit n de $\mathbb{N}^*$, $3 \times 5^{2n-1} + 2^{3n-2}$ est divisible par 17.

1.26* Soit $(u_n)_{n \in \mathbb{N}}$ une suite d'entiers naturels strictement croissante.

a) Démontrer que l'ensemble des valeurs de cette suite est non majoré.

b) Démontrer que pour tout entier naturel $x \geqslant u_0$ il existe un entier naturel unique n tel que :

$$u_n \leqslant x < u_{n+1}.$$

Appliquer ce résultat aux suites définies pour tout n par $u_n = a^n$ (a entier > 1), $v_n = n!$ ($n > 0$).

1.27 *a*) Démontrer que pour tout $n > 0$ on a

$$n \leqslant n! \leqslant n^n$$

b)* Démontrer que pour tout entier $a > 1$ il existe un entier p tel que

$$\forall n \in]p, +\infty[\quad a^n < n!$$

(Pour $n \geqslant a$ on pourra écrire $n! = (1.2 \ldots a - 1)[a(a+1) \ldots n]$)

1.28* On désigne par F l'ensemble des suites *finies* ne prenant que les valeurs 1 et 2. On désignera une telle suite par $(k_1, k_2 \ldots, k_p)$; par exemple (1), (2), (1, 1), (1, 2, 1) (2, 2, 1, 2) etc. sont des éléments de F.

Pour tout entier naturel n, on désigne par S_n l'ensemble des suites $(k_1, \ldots, k_p)$ de F telles que

$$k_1 + k_2 + \ldots + k_p = n + 1,$$

et on pose $u_n = \text{card } S_n$. (u_n est le nombre de manières de verser n francs en versant *successivement* soit 1 franc, soit 2 francs). La suite (u_n) est appelée suite de FIBONACCI.

a) Calculer u_0, u_1, u_2, u_3.

b) On désigne par S'_{n+2} et S''_{n+2} les ensembles de suites de S_{n+2} se terminant respectivement par 1 et par 2. Démontrer que S'_{n+2} et S''_{n+2} sont complémentaires dans S_{n+2}. En déduire que pour tout n on a

$$u_{n+2} = u_{n+1} + u_n.$$

c) Démontrer qu'il existe deux nombres réels α et β tels que, pour tout n, on ait

$$u_{n+2} - \alpha u_{n+1} = \beta (u_{n+1} - \alpha u_n).$$

d) En utilisant la relation précédente démontrer que $u_{n+1} - \alpha u_n = \beta^n (u_1 - \alpha u_0)$.
Calculer $u_{n+1} - \alpha u_n$ en fonction de β et de n et, de même, $u_{n+1} - \beta u_n$ en fonction de α et de n.
En déduire la valeur de u_n à l'aide de α, β, n.

1.29 *a*) Pour tout entier naturel n, trouver le nombre des solutions $(x, y) \in \mathbb{N} \times \mathbb{N}$ de l'équation $x + y = n$.

b) Même question pour $x + 2y = n$.

1.30 Pour tout entier naturel n, trouver le nombre de solutions $(x, y, z) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ de l'équation $x + y + z = n$. (Utiliser le *a* de l'exercice 29.)

1.31 *a*) Démontrer par récurrence que, si un ensemble E a n éléments, alors $\mathfrak{T}$ (E) a 2^n éléments (on pourra poser $E_{n+1} = E_n \cup \{a\}$ avec $a \notin E_n$).

b) Un ensemble E étant donné, on appelle fonction caractéristique, φ_A, de la partie A de E, l'application de E dans {0, 1} telle que $\varphi_A(x) = 0$ pour tout x de E — A et $\varphi_A(x) = 1$ pour tout x de A.
Démontrer que l'application $A \longrightarrow \varphi_A$ de $\mathfrak{T}$ (E) dans $\mathcal{F}$ (E, {0, 1}) est une bijection.
Retrouver ainsi le cardinal de $\mathfrak{T}$ (E) pour E fini.

1.32* On donne n points distincts $A_1, \ldots, A_n$ d'un plan, trois quelconques de ces points n'étant pas alignés.

a) Soit $\mathfrak{D}$ l'ensemble des droites D joignant les points $A_1 \ldots A_n$ deux à deux. Calculer le nombre d de ces droites.

b) On suppose que les points $A_1 \ldots A_n$ sont choisis de manière que, quels que soient les entiers i, j, k, l tous distincts de [1 , n], les droites (A_iA_j) et (A_kA_l) soient sécantes.
Combien de droites D passent par un point A_i?
Pour combien d'unités compte le point A_i dans le calcul du nombre des points d'intersection des droites D deux à deux?

c) Calculer le nombre total p des points d'intersection des droites D deux à deux, distincts des points donnés $A_1 \ldots A_n$.

d) Écrire p sous la forme d'un coefficient binomial.
Retrouver directement ce résultat en calculant p pour $n = 4$.

1.33 Démontrer que, quels que soient les entiers naturels n et p, tels que $p \leqslant n$, on a

$$C_p^p + C_{p+1}^p + \ldots + C_n^p = C_{n+1}^{p+1},$$

a) par récurrence;

b) en écrivant $C_{k+1}^{p+1} = C_k^{p+1} + C_k^p$ pour $p + 1 \leqslant k \leqslant n$.

1.34 Démontrer que, quels que soit $n \geqslant 2$, on a

$$C_n^p = C_{n-2}^p + 2\,C_{n-2}^{p-1} + C_{n-2}^{p-2}$$

a) par un calcul direct;

b) en comptant pour un ensemble E de cardinal n le nombre des parties ayant p éléments

- contenant a et b,
- contenant a ou bien b,
- ne contenant ni a, ni b,

a et b étant deux éléments distincts de E.

1.35 Calculer $S = \frac{1}{1} C_n^0 + \frac{1}{2} C_n^1 + \ldots + \frac{1}{n+1} C_n^n$.

$\left(\text{On remarquera que } C_{n+1}^p = \frac{n+1}{p} C_n^{p-1}\right)$.

1.36 Calculer $S' = C_n^1 + 2\,C_n^2 + \ldots + n\,C_n^n$.

$\left(\text{On remarquera que } C_n^p = \frac{n}{p} C_{n-1}^{p-1}\right)$.

1.37 Calculer, en utilisant les coefficients binomiaux,

$$A = 1 \times 2 \ldots p + 2 \times 3 \ldots (p+1) + \ldots + n\,(n+1) \ldots (n-p+1).$$

1.38 Existe-t-il un système de numération dans lequel on a

$$\overline{41} \times \overline{14} = \overline{1224}?$$

Même question avec

$$\overline{52} \times \overline{25} = \overline{1693}.$$

1.39 Déterminer la base du système de numération dans lequel on a

$$\overline{46} + \overline{53} = \overline{132}$$

et effectuer, dans ce système, l'opération $\overline{46} \times \overline{53}$.

1.40 Trouver la base du système de numération pour laquelle on a

$$\overline{35} + \overline{13} = \overline{51}.$$

Comment les trois termes de cette égalité s'écrivent-ils dans le système de base deux?

1.41 Un nombre s'écrit 1 101 010 011 dans le système binaire. Écrire ce nombre dans le système de base huit.

1.42 Établir les tables d'addition et de multiplication dans le système de numération de base 12.
(Les symboles sont : 0, 1, 2, ..., 9, α, β).
Effectuer les opérations suivantes :

$$\overline{2\,\alpha\,34} + \overline{1\,\beta\alpha\,07};$$
$$\overline{\beta\,012\,\alpha} - \overline{\alpha\,867};$$
$$\overline{3\,\alpha\,5} \times \overline{87};$$
$$\overline{48\,\alpha\,3} : 9;$$
$$\overline{503\,\beta\alpha} : \overline{\alpha\,7}.$$

1.43 Quels sont les nombres de trois chiffres qui s'écrivent $\overline{xyz}$ dans le système de base 7 et zyx dans le système de base 11?

1.44 Dans quel système de numération $(13)^4$ s'écrit-il $\overline{14641}$?

1.45 Dans le système de numération de base x, les chiffres a et b sont consécutifs. Peut-on déterminer a, b, x de telle sorte que :

$$\overline{aaaa} = (\overline{bb})^2?$$

1.46 Les nombres a, b, c sont des nombres entiers appartenant à l'ensemble

$$\{0, 1, 2, 3, 4\}.$$

On représente par abc le nombre $5^2\,a + 5\,b + c$.
Démontrer que $\overline{abc}$ est divisible par 4 si, et seulement si $a + b + c$ est divisible par 4.
Démontrer que $\overline{abc}$ est divisible par 6 si, et seulement si $a - b + c$ est divisible par 6.

1.47 Dans le système de numération de base douze, on écrit, les uns à la suite des autres, les nombres de 1 à n. Quel est le 150^e chiffre écrit?

1.48 1° Dans un système de base x ($x > 2$), démontrer que les nombres :

$$N = (x - 1)^2 \quad \text{et} \quad P = 2\,(x - 1)$$

s'écrivent respectivement $\overline{ab}$ et $\overline{ba}$.

2° Dans un système de base x ($x > 3$), démontrer que les nombres :

$$Q = (x - 1)^3 \quad \text{et} \quad R = (x + 2)\,(x - 1)^2$$

s'écrivent avec les mêmes chiffres.

3° On suppose que p et q sont deux nombres entiers naturels tels que

$$p + q = x + 1$$

et qu'ils n'appartiennent pas à l'ensemble $\{0, 1, x\}$.
Démontrer que, dans le système de numération de base x, les deux nombres

$$S = p\,(x - 1) \quad \text{et} \quad T = q\,(x - 1)$$

s'écrivent avec les mêmes chiffres.

1.49 On considère le nombre entier $\overline{aabb}$ écrit dans le système décimal. Existe-t-il des chiffres a et b tels que ce nombre soit un carré?

1.50 Dans le système de numération de base x, les chiffres a et b sont consécutifs. Peut-on déterminer a, b, x de telle sorte que

$$\overline{aaaa} = (\overline{bb})^2?$$

1.51 Dans le système de numération de base dix, déterminer un nombre de quatre chiffres dont le produit par 3 se termine par 4235.
Dans le système de numération de base dix, déterminer un nombre de quatre chiffres dont le produit par 4 se termine par 7856.
Dans le système de numération de base dix, déterminer un nombre de quatre chiffres dont le produit par 27 se termine par 1245.
Dans le système de numération de base dix, déterminer un nombre de trois chiffres dont le produit par 793 se termine par 801.
Dans le système de numération de base dix, déterminer un nombre de trois chiffres dont le produit par 378 se termine par 786.

1.52 Dans le système de numération de base dix, déterminer tous les nombres compris entre 1500 et 2500 et qui, divisés par 45 donnent un quotient égal au reste.

1.53 Dans le système de numération de base dix, on effectue une division : le dividende est égal à 353 et le reste est 5. Quels peuvent être le diviseur et le quotient?

1.54 On divise un nombre a par un nombre b. On trouve pour quotient 109 et pour reste 3057. Combien d'unités peut-on ajouter à la fois au dividende et au diviseur pour ne pas modifier le quotient?

1.55 Déterminer tous les nombres de deux chiffres qui sont divisibles par le produit de leurs chiffres.

1.56 A quelle condition un nombre N peut-il représenter la somme de p nombres consécutifs? Applications

$p = 3$, $N = 162$; $p = 4$, $N = 534$; $p = 5$, $N = 1015$; $p = 6$, $N = 858$.

1.57 Dans le système de numération de base x, deux nombres a et b ont respectivement p chiffres et q chiffres. Combien le produit ab peut-il avoir de chiffres?

1.58 Dans le système de numération de base dix, on écrit les nombres de 1 à 715. On supprime tous ceux où figure le chiffre 3. Combien en reste-t-il? Quel rang occupe le nombre 428? Quel est le 400^{e} nombre écrit?

1.59 Dans le système de numération de base dix, on écrit, les uns à la suite des autres, les nombres de 1 à n. On a utilisé en tout 3333 chiffres. Que vaut n?

1.60 Dans le système de numération de base dix, on écrit, les uns à la suite des autres, les nombres de 1 à 734. Combien utilise-t-on de chiffres? Combien de fois utilise-t-on chacun des chiffres?

1.61 1° Combien de nombres s'écrivent, dans le système de base dix, avec 3 chiffres distincts)? (Le chiffre des centaines est supposé non nul.)

2° Quelle est la somme de ces nombres?

1.62 1° Avec les chiffres 1, 2, 3, 4, 5, 6 combien peut-on écrire de nombres de 6 chiffres distincts?

2° Quelle est la somme de ces nombres?

3° On range ces nombres dans l'ordre croissant; quel est le 550^{e} nombre?

4° Avec les mêmes chiffres 1, 2, 3, 4, 5, 6, combien peut-on écrire de nombres de 3 chiffres distincts? Quelle est la somme de ces nombres?

Sujets d'étude.

1.63 Soit a un entier naturel tel que $a \geqslant 2$.

a) Démontrer que pour tout $x \in \mathbb{N}^*$ il existe un entier naturel k unique tel que $a^k \leqslant x < a^{k+1}$. (Utiliser ex. 1.16 et 1.26).

b) Démontrer que pour tout x de $\mathbb{N}^*$ il existe un entier naturel unique k et un entier naturel unique x_k vérifiant $0 \leqslant x_k < a$ tels que

$$x_k\, a^k \leqslant x < (x_k + 1)\, a^k.$$

c) Déduire de ce qui précède que, pour tout x de $\mathbb{N}$, il existe un entier naturel unique n et une suite unique $(x_k)_{0 \leqslant k \leqslant n}$ d'entiers naturels de $[0\,,\, a-1]$ tels que

$$x = x_n\, a^n + \ldots + x_1\, a + x_0.$$

1.64 On se propose de montrer que $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$ sont équipotents. Pour cela on considère l'application f de $\mathbb{N} \times \mathbb{N}$ définie par

$$\begin{aligned} f(0,0) &= 0 \\ f(0,y) &= f(y-1,0) + 1 \qquad \text{pour tout } y \geqslant 1 \\ f(x,y) &= f(x-1,y+1) + 1 \quad \text{pour tout } x \geqslant 1 \text{ et tout } y. \end{aligned}$$

On appellera segment S_k l'ensemble des couples d'entiers naturels (x, y) tels que $x + y = k$ $(k \in \mathbb{N})$.

a) Quel est le cardinal de S_k? Calculer $f(x, y)$ en fonction de x et y.

b) Quel que soit l'entier naturel n, démontrer qu'il existe un entier naturel unique k tel que

$$\frac{k(k+1)}{2} \leqslant n < \frac{(k+1)(k+2)}{2}.$$

(On pourra utiliser l'exercice 1.26 ou montrer que, si α est la racine positive de $\frac{x(x+1)}{2} = n$, on a $\alpha - 1 < k \leqslant \alpha$.)

c) Quel que soit l'entier naturel n, démontrer que l'équation $f(x, y) = n$ a une solution unique. (On cherchera a déterminer le rang k du segment S_k auquel appartient (x, y)). En déduire que f est bijective.

Application numérique : Calculer (x, y) pour $n = 10\,000$.

1.65 On se propose de calculer le nombre des *surjections* d'un ensemble E_n dans un ensemble E_p de cardinaux respectifs n et p, entiers naturels *non nuls*.
Soit $S_{n,p}$ l'ensemble de ces surjections; on pose

$$f(n, p) = \text{card } S_{n,p}.$$

a) Que peut-on dire de n et p lorsque $f(n, p) \neq 0$? On fera cette hypothèse dans toute la suite.
Quelles sont les valeurs de $f(n, 1)$ et $f(n, n)$?

b) On suppose $n \geqslant 2$; on choisit une fois pour toute $a \in E_n$ et on pose $E' = E_n - \{a\}$. Désignant par $b_1, b_2, \ldots, b_p$ les éléments de F_p, pour tout i de $[1\ ,\ p]$, on pose

$$\begin{aligned} S_i &= \{ s \in S_{n,p} \mid s(a) = b_i \}, \\ S'_i &= \{ s \in S_i \mid b_i \notin s(E') \}, \\ S''_i &= \{ s \in S_i \mid b_i \in s(E') \}. \end{aligned}$$

Calculer les cardinaux de S'_i et de S''_i en utilisant certains des nombres $f(h, k)$ pour h et k convenablement choisis; en déduire le cardinal de S_i.

c) Démontrer que la suite $(S_i)_{1 \leqslant i \leqslant p}$ définit une partition de $S_{n,p}$; en déduire que l'on a

$$f(n, p) = p\,(f(n-1, p-1) + f(n-1, p)).$$

Application numérique : Calculer $f(3, 2)$, $f(4, 2)$, $f(4, 3)$, $f(5, 2)$, $f(5, 3)$, $f(5, 4)$.

d) On désigne par $g(n, p)$ le nombre des partitions de E_n, comprenant p parties. Démontrer que

$$g(n, p) = \frac{1}{p!} f(n, p).$$

2| Entiers relatifs.

Les propriétés des entiers relatifs sont exposées dans ce chapitre en quatre sections :
Section I. *Groupe additif* $(\mathbb{Z}, +)$ *et groupe totalement ordonné* $(\mathbb{Z}, +, \leqslant)$. *Anneau* $(\mathbb{Z}, +, \times)$ *et anneau totalement ordonné* $(\mathbb{Z}, +, \times, \leqslant)$.
Section II. *Sous-groupes du groupe* $\mathbb{Z}$, *idéaux de l'anneau* $\mathbb{Z}$; *entiers modulo* n.
Section III. *Divisibilité dans l'anneau* $\mathbb{Z}$; p.g.c.d. *et* p.p.c.m. *de deux ou plusieurs entiers.*
Section IV. *Nombres premiers.*

Ce chapitre est d'abord important parce qu'il développe les propriétés des entiers relatifs qui sont utilisées dans beaucoup de théories mathématiques. Mais il l'est à un autre titre; en effet, la considération du groupe $\mathbb{Z}$, *des anneaux* $\mathbb{Z}$ *et* $\mathbb{Z}/n\mathbb{Z}$ *permet de revoir certaines notions étudiées dans les classes précédentes (loi interne, partie stable, groupe, sous-groupe, anneau, sous-anneau, corps) mais encore de préciser certaines notions déjà entrevues et d'étudier des notions nouvelles (idéal d'un anneau commutatif, loi interne compatible avec une relation d'équivalence, homomorphismes et isomorphismes).*

Le contenu de ce chapitre ne fait pas partie du programme de la **Section E.** *Chaque fois que nous utiliserons dans les chapitres suivants une notion dont la définition est donnée ou rappelée dans ce chapitre* 2, *nous indiquerons explicitement l'endroit où l'élève de la Section E pourra retrouver cette définition.*

I. Anneau totalement ordonné $(\mathbb{Z}, +, \times, \leqslant)$

2. 1 GROUPE $(\mathbb{Z}, +)$

a) Rappels.

Définition.

On dit que l'ensemble G muni d'une loi interne notée $\star$, c'est-à-dire $(G, \star)$ est un **groupe** si et seulement si

G_1. La loi interne est associative.
G_2. La loi interne possède un élément neutre dans G.
G_3. Tout élément de G possède un symétrique dans G.

Si on a, de plus :

G_C. La loi interne est commutative,
on dit que le groupe $(G, \star)$ est **commutatif.**

Rappelons que pour toute loi interne possédant un élément neutre, **cet élément neutre est unique.** En notation additive l'élément neutre est appelé **élément zéro** et en notation multiplicative **élément unité.**

Rappelons également que, pour toute loi interne associative, possédant un élément neutre, si un élément x possède un symétrique, **ce symétrique est unique.** En notation additive le symétrique de x, appelé **opposé** de x, se note $-x$ et en notation multiplicative le symétrique de x, appelé **inverse** de x se note x^{-1}.

Rappelons enfin, qu'étant donné un ensemble E muni d'une loi interne notée $\star$, on appelle **partie stable** de E pour la loi $\star$ toute partie S de E telle que

$$(\forall (x,\ y) \in S \times S) \qquad x \star y \in S.$$

On définit ainsi une loi interne sur S appelée **loi induite** sur S par la loi définie sur E. En général il n'y a aucun inconvénient à noter par le même symbole la loi sur E et la loi induite.
On dit aussi que la loi définie sur E **prolonge** la loi définie sur S.

b) Groupe $(\mathbb{Z}, +)$.

Nous admettrons le résultat suivant :

Il existe un ensemble $\mathbb{Z}$ appelé ensemble des **entiers relatifs** (on dit aussi **entiers rationnels**) muni d'une addition tel que
i. $(\mathbb{Z}, +)$ est un groupe commutatif.
ii. $\mathbb{N}$ est une partie stable de $\mathbb{Z}$ pour l'addition.
iii. Il n'existe pas d'ensemble G strictement inclus dans $\mathbb{Z}$ possédant les propriétés *i* et *ii*.

REMARQUE 1

Nous admettrons que, si $(\mathbb{Z}, +)$ et $(\mathbb{Z}', +)$ possèdent les trois propriétés ci-dessus, alors ces groupes sont isomorphes; c'est-à-dire qu'il existe une application

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}'$$
$$x \longmapsto x'$$

telle que

$$(\forall (x, y) \in \mathbb{Z} \times \mathbb{Z}) \qquad f(x + y) = f(x) + f(y).$$

Le groupe $\mathbb{Z}$ contient $\mathbb{N} = \{0, 1, 2, \ldots\}$ il contient également l'ensemble des opposés des éléments de $\mathbb{N}$ que nous noterons $-\mathbb{N}$; donc $-\mathbb{N} = \{0, -1, -2, \ldots\}$; nous admettrons que

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}).$$

D'autre part, soit $x \in \mathbb{N} \cap (-\mathbb{N})$; alors $x \in \mathbb{N}$ et $x \in -\mathbb{N}$, donc $-x \in \mathbb{N}$; x et $-x$ appartenant à $\mathbb{N}$ on a $x = 0$; donc

$$\mathbb{N} \cap (-\mathbb{N}) = \{0\}.$$

Posant $\mathbb{N}^* = \mathbb{N} - \{0\}$ et désignant par $-\mathbb{N}^*$ l'ensemble des opposés des éléments de $\mathbb{N}^*$, on voit que

$$\mathbb{N}^* \ , \ \{0\} \ , \ -\mathbb{N}^*$$

constituent une *partition* de $\mathbb{Z}$. Il en est de même de $\mathbb{N}$ et $-\mathbb{N}^*$ et de $\mathbb{N}^*$ et $-\mathbb{N}$.

Le lecteur qui le désire trouvera les démonstrations des résultats énoncés ci-dessus dans l'Annexe C à la fin du livre.

c) Règles de calcul dans le groupe $(\mathbb{Z}, +)$.

Ce sont les règles de calcul dans tout groupe commutatif. Ces règles sont rappelées pour $\mathbb{Z}$; vous les démontrerez à titre d'exercice.

Propriété 1.

Comme dans tout ensemble muni d'une loi interne on a, quels que soient x, y, z,

(1) $$(x = y) \Longrightarrow (x + z = y + z).$$

Le fait que $\mathbb{Z}$ est un groupe entraîne que l'on a aussi

(1′) $$(x + z = y + z) \Longrightarrow (x = y).$$

(Ajouter $-z$ aux deux membres de $x + z = y + z$ et appliquer (1)).

Propriété 2.

Quels que soient a et b de $\mathbb{Z}$, il existe un entier relatif unique x tel que

(2) $$x + a = b.$$

Cet entier unique est $b + (-a)$ que l'on note $b - a$; il est appelé différence de b et a. (Ajouter $-a$ aux deux membres de (2)).

Propriété 3.

Quels que soient x et y de $\mathbb{Z}$, on a

$$-(x + y) = (-x) + (-y).$$

(On sait que l'opposé de $x + y$ existe et est unique; vérifier que $(-x) + (-y)$ est bien l'opposé de $x + y$).
L'entier relatif $(-x) + (-y)$ s'écrit plus simplement $-x - y$.

REMARQUE 2

Dans un groupe non commutatif, si x' et y' sont les symétriques de x et y dans $(G, \star)$ rappelons que l'on a

$$(x \star y)' = y' \star x'$$

Par exemple dans l'ensemble $\mathfrak{B}(E, E)$ des bijections d'un ensemble quelconque E sur lui-même, muni de la composition des applications on a

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

2. 2 GROUPE TOTALEMENT ORDONNÉ $(\mathbb{Z}, +, \leqslant)$

a) Introduction.

Nous allons démontrer qu'il existe sur $\mathbb{Z}$ une *relation d'ordre total unique* telle que :

i. Sur la partie stable $\mathbb{N}$ *cette relation d'ordre total se réduit à la relation notée* $\leqslant$ *sur* $\mathbb{N}$.
Il n'y aura donc aucun inconvénient à noter de même $\leqslant$ la relation d'ordre total sur $\mathbb{Z}$.

ii. La relation d'ordre sur $\mathbb{Z}$ *et l'addition définie sur* $\mathbb{Z}$ *sont compatibles; c'est-à-dire, quels que soient* x, y, z *de* $\mathbb{Z}$, *on a*

(1) $$(x \leqslant y) \Longrightarrow (x + z \leqslant y + z).$$

Si on a (1), en ajoutant $-z$ aux deux membres de $x + z \leqslant y + z$, on voit que, quels que soient x, y, z on a

(1′) $$(x + z \leqslant y + z) \Longrightarrow (x \leqslant y).$$

Si la relation d'ordre et l'addition sur $\mathbb{Z}$ sont compatibles, on a donc, quels que soient x, y, z de $\mathbb{Z}$

$$(x \leqslant y) \Longleftrightarrow (x + z \leqslant y + z).$$

Supposons qu'il existe sur $\mathbb{Z}$ une relation d'ordre total possédant les propriétés *i* et *ii*. Quels que soient x, y de $\mathbb{Z}$ on a

$$(x \leqslant y) \Longleftrightarrow (0 \leqslant y - x).$$

Quel que soit a de $\mathbb{N}$ on a $0 \leqslant a$ dans $\mathbb{N}$; cette relation est encore vraie dans $\mathbb{Z}$ (propriété *i*); d'où, en appliquant la propriété *ii*, on aura

$$0 + (-a) \leqslant a + (-a) \quad \text{c'est-à-dire} \quad -a \leqslant 0.$$

Or $a \in \mathbb{N}$ et $-a \in -\mathbb{N}$ donc quel que soit a de $\mathbb{Z}$ on a

$$(0 \leqslant a) \Longleftrightarrow (a \in \mathbb{N}).$$

Il en résulte que, si la relation que nous cherchons existe, on a, quels que soient x et y de $\mathbb{Z}$,

$$(x \leqslant y) \Longleftrightarrow (y - x \in \mathbb{N}).$$

b) Étude de la relation $y - x \in \mathbb{N}$ définie sur $\mathbb{Z}$.

Quel que soit l'entier relatif x, on a

$$x - x = 0 \in \mathbb{N}.$$

Soient deux entiers relatifs quelconques x et y; on a

$$-(y - x) = -[y + (-x)] = -y - (-x) = x - y.$$

Si $y - x \in \mathbb{N}$ et $x - y \in \mathbb{N}$, alors $y - x \in \mathbb{N}$ et $y - x \in -\mathbb{N}$; donc $y - x \in \mathbb{N} \cap (-\mathbb{N}) = \{0\}$, ou encore $x = y$. Par conséquent quels que soient les entiers relatifs x et y, on a

$$(y - x \in \mathbb{N} \quad \text{et} \quad x - y \in \mathbb{N}) \Longrightarrow (x = y).$$

Enfin quels que soient les entiers relatifs x, y, z, on a

$$(y - x) + (z - y) = z - x.$$

Comme $a \in \mathbb{N}$ et $b \in \mathbb{N}$ implique $a + b \in \mathbb{N}$, on a

$$(y - x \in \mathbb{N} \quad \text{et} \quad z - y \in \mathbb{N}) \Longrightarrow (z - x \in \mathbb{N}).$$

La relation $y - x \in \mathbb{N}$ est donc une *relation d'ordre* définie sur $\mathbb{Z}$.

Comme $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$, quels que soient x et y, l'entier relatif $y - x$ appartient à $\mathbb{N}$ ou à $-\mathbb{N}$; on a donc $y - x \in \mathbb{N}$ ou $x - y \in \mathbb{N}$; l'ordre défini sur $\mathbb{Z}$ par la la relation $y - x \in \mathbb{N}$ est donc *total*.

Enfin quels que soient les entiers relatifs x, y, z, on a

$$y - x = (y + z) - (x + z)$$

donc

$$(y - x \in \mathbb{N}) \Longrightarrow ((y + z) - (x + z) \in \mathbb{N}).$$

La relation d'ordre définie sur $\mathbb{Z}$ par $y - x \in \mathbb{N}$ et l'addition dans $\mathbb{Z}$ sont *compatibles*.

Résumons notre étude : nous avons vu que, s'il existe sur $\mathbb{Z}$ une relation d'ordre total vérifiant les propriétés *i* et *ii*, ce ne peut être que la relation $y - x \in \mathbb{N}$. Or cette relation est une relation d'ordre total sur $\mathbb{Z}$, compatible avec l'addition de $\mathbb{Z}$; pour les éléments de $\mathbb{Z}$ appartenant à $\mathbb{N}$ elle se réduit manifestement à $x \leqslant y$ sur $\mathbb{N}$. Concluons :

Théorème.

Il existe une seule relation d'ordre total sur $\mathbb{Z}$ telle que

i. Cette relation se réduise à la relation notée $\leqslant$ sur $\mathbb{N}$.

ii. Cette relation d'ordre total et l'addition de $\mathbb{Z}$ soient compatibles.

Cette relation est définie, quels que soient x et y de $\mathbb{Z}$, par

$$y - x \in \mathbb{N}.$$

Nous la noterons $x \leqslant y$, donc

$$(\forall\, (x, y) \in \mathbb{Z} \times \mathbb{Z}) \qquad (x \leqslant y) \iff (y - x \in \mathbb{N}).$$

Nous résumerons ces propriétés en disant que $(\mathbb{Z}, +, \leqslant)$ est un **groupe commutatif totalement ordonné.**

Notons en particulier que l'on a, pour tout x de $\mathbb{Z}$,

$$(0 \leqslant x) \iff (-x \leqslant 0).$$

REMARQUE 1

D'une manière générale on dit que $(G, +, \leqslant)$ est un *groupe commutatif totalement ordonné* si et seulement si

i. $(G, +)$ est un *groupe commutatif.*

ii. $(G, \leqslant)$ est un *ensemble totalement ordonné.*

iii. Ces deux structures sont *compatibles*, c'est-à-dire, quels que soient x, y, z de G, on a

$$(x \leqslant y) \Longrightarrow (x + z \leqslant y + z).$$

Si la troisième propriété n'était pas vérifiée on pourrait faire des calculs dans $(G, +)$, dans $(G, \leqslant)$ mais on ne pourrait faire de calculs mettant en jeu *à la fois* l'ordre et l'addition.

c) Notations et vocabulaire.

La relation $x \leqslant y$ se lit « x est **inférieur** à y ».

La relation $(x \leqslant y \quad \text{et} \quad x \neq y)$ s'écrit $x < y$ et se lit « x est **strictement inférieur** à y ».

La relation $x \geqslant y$ signifie $y \leqslant x$ et se lit « x est **supérieur** à y ».

La relation $x > y$ signifie $y < x$ et se lit « x est **strictement supérieur** à y ».

REMARQUE 2

Il est évident que les relations notées $\geqslant$ et $>$ sont les relations réciproques respectives des relations notées $\leqslant$ et $<$.

Il peut être avantageux de s'imposer la discipline de n'utiliser que les symboles $\leqslant$ et $<$, sans renoncer toutefois aux locutions « supérieur à » ou « strictement supérieur à ».

EXERCICE

Démontrer que, quels que soient les entiers relatifs x, y, z, on a

$$(x < y) \iff (x + z < y + z).$$
$$(0 < x) \iff (-x < 0).$$

L'entier relatif x est **positif** si et seulement si $0 \leqslant x$.
— x — **strictement positif** — $0 < x$.
— x — **négatif** — $x \leqslant 0$.
— x — **strictement négatif** — $x < 0$.

Quel que soit l'entier relatif x on appelle **valeur absolue de** x et on note $|x|$ le plus grand des deux entiers x et $-x$; $|x|$ est donc un *entier positif*; on écrit

$$|x| = \sup(x, -x).$$

On a donc

$$|x| = \begin{cases} x & \text{si } 0 \leqslant x, \\ -x & \text{si } x \leqslant 0. \end{cases}$$

Quel que soit x de $\mathbb{Z}$ on a $|-x| = |x|$.
Cette définition montre enfin que, quel que soit l'entier relatif x, on a

$$(x = 0) \iff (|x| = 0).$$

d) Parties non vides majorées ou minorées de $\mathbb{Z}$.

Soit A une partie non vide majorée de $\mathbb{Z}$ (cf. § 1. 1). Désignons par A′ l'ensemble des éléments positifs de A; on a donc $A' = A \cap \mathbb{N}$.

Si $A' \neq \varnothing$, A′ est une partie majorée non vide de $\mathbb{N}$, elle a donc (cf. § 1. 2) un *plus grand élément* a; cet élément a appartient à $A' \subset A$ donc à A, la transitivité de la relation $\leqslant$ montre que a est aussi le plus grand élément de A.
Si $A' = \varnothing$ tous les éléments de A sont strictement négatifs; donc ceux de — A, ensemble des opposés des éléments de A, sont strictement positifs; — A est donc une partie non vide de $\mathbb{N}$, elle a (cf. § 1. 2) un plus petit élément que nous notons $-b$. Quel que soit x de A on a donc $-b \leqslant -x$ et $-b \in -A$, d'où $x \leqslant b$ et $b \in A$: A a donc un plus grand élément.
On montrerait de même que toute partie minorée non vide de $\mathbb{Z}$ a un plus petit élément.

Théorème.

Toute partie majorée (resp. minorée) non vide de $\mathbb{Z}$ a un plus grand (resp. petit) élément.

2. 3 ANNEAU $(\mathbb{Z}, +, \times)$

a) Rappels.

Définition.

On dit que l'ensemble A muni de deux lois internes, la première notée additivement, la deuxième multiplicativement, est un **anneau** si et seulement si

i. (A, +) est un groupe commutatif.
ii. La multiplication est associative.
iii. La multiplication est distributive par rapport à l'addition, c'est-à-dire que, quels que soient x, y, z de A on a

D_1 $\quad x(y + z) = xy + xz.$
D_2 $\quad (y + z)x = yx + zx.$

Comme vous le savez, le produit $x \times y$ de x et y se note aussi $x.y$ et plus simplement xy.

L'élément neutre de l'addition est appelé l'**élément zéro** ou le **zéro** de l'anneau A; on peut le noter 0_A.

Si la *multiplication* possède un *élément neutre e*, on dit que *e* est l'**élément unité** de l'anneau A qui est alors appelé **anneau unitaire.**

Si la *multiplication* est commutative dans A on dit que A est un **anneau commutatif.**

EXERCICE 1

Expliciter les axiomes de la structure d'anneau, puis ceux de la structure d'anneau commutatif unitaire.

b) Définition d'une multiplication dans $\mathbb{Z}$.

Nous allons montrer qu'il existe dans l'ensemble $\mathbb{Z}$ des entiers relatifs une *loi interne unique* appelée *multiplication* possédant les deux propriétés suivantes :

i. La multiplication définie dans $\mathbb{Z}$ prolonge la multiplication définie dans $\mathbb{N}$, partie de $\mathbb{Z}$.

ii. Cette multiplication est distributive par rapport à l'addition dans $\mathbb{Z}$.

Exceptionnellement dans ce sous-paragraphe *b)* nous noterons $a, b, \ldots, x, \ldots$ les éléments de $\mathbb{N}$ et $-a, -b, \ldots, -x, \ldots$ les éléments de $-\mathbb{N}$.

Quels que soient a et b de $\mathbb{N}$ nous connaissons déjà ab. Comme $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ la multiplication dans $\mathbb{Z}$ sera définie lorsque nous saurons calculer

$$(-a)\,b \quad , \quad a\,(-b), \quad (-a)\,(-b).$$

Les entiers naturels a et b étant quelconques, s'il existe une multiplication dans $\mathbb{Z}$ possédant les propriétés *i* et *ii* on aura

$$[a + (-a)]\,b = 0.b = 0,$$

donc (propriété *ii*)

$$ab + (-a)\,b = 0;$$

et, enfin, d'après l'unicité de l'opposé de x dans $(\mathbb{Z}, +)$:

$$(-a)\,b = -(ab).$$

En calculant $a\,[b + (-b)]$ on trouvera de même que $a\,(-b) = -(ab)$.

On aura enfin, toujours quels que soient les entiers naturels a et b,

$$[a + (-a)]\,(-b) = 0.(-b) = -(0.b) = -0 = 0$$

donc (propriété *ii*)

$$a\,(-b) + (-a)\,(-b) = 0$$

et enfin, comme nous venons de voir que $a\,(-b) = -(ab)$

$$(-a)\,(-b) = -[(a\,(-b)] = -[-(ab)] = ab.$$

Donc s'il existe une multiplication dans $\mathbb{Z}$ possédant les propriétés *i* et *ii* on a, quels que soient a et b de $\mathbb{N}$,

le produit de a et b est ab,
— $(-a)$ et b est $-(ab)$,
— a et $(-b)$ est $-(ab)$,
— $(-a)$ et $(-b)$ est ab.

Considérons la multiplication ainsi définie; elle *prolonge* la multiplication définie sur $\mathbb{N}$.

Elle est visiblement *commutative*. Montrons qu'elle est *distributive par rapport à l'addition*. Avec les notations utilisées, l'addition étant commutative, nous aurons 6 cas à examiner

(1) $c\,(a+b)$ (2) $(-c)\,(a+b)$
(3) $c\,[a+(-b)]$ (4) $(-c)\,[a+(-b)]$
(5) $c\,[(-a)+(-b)]$ (6) $(-c)\,[(-a)+(-b)]$

Pour le cas (1) c'est la distributivité dans $\mathbb{N}$. La distributivité dans les cas (2), (5) et (6) se vérifie immédiatement en utilisant la définition de la multiplication, les propriétés de $(\mathbb{Z}, +)$ et la distributivité dans $\mathbb{N}$; en effet

$$(-c)\,[a+b] = -\,[c\,(a+b)] = -\,(ca+cb) = (-ca)+(-cb) = (-c)\,a+(-c)\,b,$$

$$c\,[(-a)+(-b)] = c\,[-\,(a+b)] = -\,[c\,(a+b)] = -\,(ca+cb) = (-ca)+(-cb),$$
$$= c\,(-a)+c\,(-b),$$

$$(-c)\,[(-a)+(-b)] = (-c)\,[-\,(a+b)] = c\,(a+b)$$
$$= ca+cb = (-c)\,(-a)+(-c)\,(-b).$$

Pour le cas 3 il faudra distinguer deux sous cas $b \leqslant a$ et $a \leqslant b$.
Si $b \leqslant a$, $a-b \in \mathbb{N}$ et dans $\mathbb{N}$ la multiplication est distributive par rapport à la soustraction, d'où

$$c\,[a+(-b)] = c\,(a-b) = ca-cb = ca+c\,(-b).$$

Si $a \leqslant b$, $a-b \notin \mathbb{N}$ mais $b-a = -\,(a-b) \in \mathbb{N}$ et on a

$$c\,[a+(-b)] = c\,(a-b) = c\,[-\,(b-a)] = -\,[c\,(b-a)] = -\,(cb-ca)$$
$$= -\,cb+ca = ca+c\,(-b).$$

En distinguant encore les deux cas $b \leqslant a$ et $a \leqslant b$ vous démontrerez à titre d'exercice que l'on a encore dans le cas (4)

$$(-c)\,[a+(-b)] = (-c)\,a+(-c)\,(-b).$$

La multiplication que nous venons de définir est donc *distributive* par rapport à l'addition. D'autre part, avec les notations adoptées, nous avons

$$|ab| = ab \quad , \quad |(-a)\,b| = |-ab| = ab \quad , \quad |(-a)\,(-b)| = |ab| = ab,$$

et

$$0 \leqslant ab \quad , \quad (-a)\,b \leqslant 0 \quad , \quad 0 \leqslant (-a)\,(-b).$$

Concluons :

Théorème.

Il existe une seule loi interne sur $\mathbb{Z}$ prolongeant la multiplication sur $\mathbb{N}$ et distributive par rapport à l'addition sur $\mathbb{Z}$.
Cette loi interne, appelée **multiplication** sur $\mathbb{Z}$, est définie de la manière suivante : Quels que soient x et y de $\mathbb{Z}$ le produit xy a pour valeur absolue le produit des valeurs absolues de x et y, ce produit est positif si x et y sont tous deux positifs ou tous deux négatifs, il est négatif si x et y sont l'un positif, l'autre négatif.

c) Anneau $(\mathbb{Z}, +, \times)$. Règles de calcul.

Désignons par $(\mathbb{Z}, +, \times)$ l'ensemble $\mathbb{Z}$ muni de l'addition définie au § 2. 1 et de la multiplication définie ci-dessus.
Nous avons vu que $(\mathbb{Z}, +)$ est un *groupe commutatif*.

Considérons trois entiers relatifs quelconques x, y, z. Les entiers $(xy)\,z$ et $x\,(yz)$ ont même valeur absolue et sont tous deux positifs ou tous deux négatifs : ils sont donc égaux. La multiplication est donc *associative*. Nous avons vu qu'elle est *commutative*. Ensuite 1 est visiblement élément neutre.
Enfin la multiplication est *distributive* par rapport à l'addition. Concluons

Théorème.

$(\mathbb{Z}, +, \times)$ est un anneau commutatif, unitaire.

La définition de la multiplication montre que quel que soit x de $\mathbb{Z}$ on a

$$0.x = x.0 = 0.$$

EXERCICE 2

Soit A un anneau quelconque, quels que soient x et y de A, calculer

$$xy = x\,(y + 0_A) \quad , \quad yx = (y + 0_A)\,x,$$

en utilisant la distributivité à gauche et à droite (axiomes D_1 et D_2). En déduire que quels que soient x de A on a

$$0_A x = x.0_A = 0_A.$$

D'autre part dans $\mathbb{Z}$, quels que soient x et y, les relations suivantes sont équivalentes :

$$xy = 0 \quad , \quad |xy| = 0 \quad , \quad |x|\,|y| = 0$$
$$|x| = 0 \quad \text{ou} \quad |y| = 0 \quad , \quad (x = 0 \quad \text{ou} \quad y = 0).$$

Théorème.

Quels que soient x et y de $\mathbb{Z}$ on a

$$xy = 0 \iff (x = 0 \quad \text{ou} \quad y = 0).$$

REMARQUE 1

Dans un anneau A quelconque il peut exister des couples (x, y) d'éléments de A tels que

$$x \neq 0_A \quad \text{et} \quad y \neq 0_A \quad \text{et} \quad xy = 0_A.$$

De tels éléments sont appelés véritables diviseurs de zéro ou plus simplement *diviseurs de zéro*.
Un anneau *commutatif dépourvu de diviseurs de zéro* est appelé *anneau intègre*.
Ainsi $\mathbb{Z}$ *est un anneau intègre*.
Nous rencontrerons au § 2.9 f des anneaux qui ne sont pas intègres.

Quels que soient les entiers relatifs x, y, z, on a

$$x\,(y - z) + xz = x\,[y + (-z)] + xz = x\,[y + (-z) + z] = x\,(y + 0) = xy$$

donc (propriété 2 du § 2. 1 *c*)

$$x\,(y - z) = xy - xz.$$

Nous dirons que dans $\mathbb{Z}$ la multiplication est *distributive* par rapport à la soustraction.
On a donc $x\,(0 - y) = x.0 - xy = -xy$ donc

$$x\,(-y) = -xy.$$

On en déduit $(-x)\,(-y) = -[(-x)\,y] = -(-xy) = xy.$

Théorème.

Quels que soient x, y, z de $\mathbb{Z}$ on a

$$x(y - z) = xy - xz,$$
$$x(-y) = (-x)y = -xy \quad , \quad (-x)(-y) = xy.$$

REMARQUE 2

Les dernières formules avaient été posées au sous-paragraphe *b* ci-dessus pour x et y *entiers naturels*, il fallait donc les démontrer pour x et y entiers relatifs quelconques.

EXERCICE 3

Soit A un anneau quelconque; démontrer que, quels que soient x, y, z de A, on a

$$x(y - z) = xy - xz \quad , \quad (y - z)x = yx - zx,$$
$$x(-y) = (-x)y = -xy \quad , \quad (-x)(-y) = xy.$$

Cherchons enfin les éléments inversibles de $\mathbb{Z}$. Quels que soient a et a' de $\mathbb{Z}$ la relation $aa' = 1$ implique $|aa'| = |a|\,|a'| = 1$. Or dans $\mathbb{N}$ le seul élément inversible est 1, concluons :

Théorème.

Les seuls éléments inversibles de $\mathbb{Z}$ sont 1 et -1.

2. 4 ANNEAU TOTALEMENT ORDONNÉ $(\mathbb{Z}, +, \times, \leqslant)$

Nous savons (cf. § 2.2 *b*) que la relation $y - x \in \mathbb{N}$ notée $x \leqslant y$ est une relation d'ordre total défini sur l'ensemble $\mathbb{Z}$.

Nous savons aussi que cette relation d'ordre est *compatible avec l'addition* c'est-à-dire que quels que soient x, y, z de $\mathbb{Z}$, on a

$$(x \leqslant y) \Longrightarrow (x + z \leqslant y + z).$$

D'autre part, d'après sa définition, la multiplication sur $\mathbb{Z}$ vérifie la propriété suivante : quels que soient x et y de $\mathbb{Z}$

$$(0 \leqslant x \quad \text{et} \quad 0 \leqslant y) \Longrightarrow (0 \leqslant xy).$$

On exprime cette propriété en disant que dans $\mathbb{Z}$ l'**ordre** $\leqslant$ et la **multiplication** sont **compatibles.**

Théorème et définition.

La relation $y - x \in \mathbb{N}$, notée $x \leqslant y$ est une relation d'ordre total défini sur $\mathbb{Z}$, elle est compatible avec l'addition et la multiplication définies sur $\mathbb{Z}$; c'est-à-dire quels que soient x, y, z on a

O.A. $\quad (x \leqslant y) \Longrightarrow (x + z \leqslant y + z)$

O.M. $\quad (0 \leqslant x \quad \text{et} \quad 0 \leqslant y) \Longrightarrow (0 \leqslant xy).$

Nous résumons ces propriétés en disant que $(\mathbb{Z}, +, \times, \leqslant)$ est un **anneau totalement ordonné.**

REMARQUE

D'une manière générale on dit que $(A, +, \times, \leqslant)$ est un anneau totalement ordonné si et seulement si

i. $(A, +, \times)$ est un *anneau commutatif,*

ii. $(A, \leqslant)$ est un *ensemble totalement ordonné,*

iii. Ces deux structures sont *compatibles;* ce qui se traduit par les énoncés OA et OM.

Si la troisième propriété n'était pas vérifiée, on pourrait faire des calculs dans $(A, \leqslant)$, dans $(A, +, \times)$ mais on ne pourrait faire des calculs mettant en jeu *à la fois* l'ordre et les opérations.

EXERCICES

1. Démontrer que, quels que soient x, y, z, de $\mathbb{Z}$ on a

$$(0 \leqslant x \text{ et } y \leqslant z) \Longrightarrow (xy \leqslant xz),$$
$$(x \leqslant 0 \text{ et } y \leqslant z) \Longrightarrow (xz \leqslant xy),$$
$$(0 < x \text{ et } y < z) \Longrightarrow (xy < xz),$$
$$(x < 0 \text{ et } y < z) \Longrightarrow (xz < xy).$$

2. Démontrer dans $\mathbb{Z}$, que, quels que soient a, b, c, d *positifs* on a

$$(a \leqslant b \text{ et } c \leqslant d) \Longrightarrow (ac \leqslant bd),$$

et que, quels que soient a, b, c, d *strictement positifs*, on a

$$(a < b \text{ et } c < d) \Longrightarrow (ac < bd).$$

3. Des relations $x \leqslant |x|$ et $-x \leqslant |x|$ vraies pour tout entier relatif, déduire que, quels que soient x, y de $\mathbb{Z}$ on a

$$|x + y| \leqslant |x| + |y|.$$

II. Sous-groupes de $(\mathbb{Z}, +)$. Idéaux de $(\mathbb{Z}, +, \times)$. Entiers modulo n.

2. 5 DIVISION EUCLIDIENNE DANS $\mathbb{Z}$

Soit a un entier relatif quelconque et b un entier relatif strictement positif.

Premier cas : $a \geqslant 0$.

Les nombres a et b sont des *entiers naturels*. Nous avons démontré au chapitre 1 qu'il existe un entier naturel unique q tel que

$$bq \leqslant a < b(q + 1).$$

Deuxième cas : $a < 0$.

Nous pouvons poser $a = -a'$, avec $a' > 0$ et appliquer à a' le résultat précédent : il existe un entier positif unique q' tel que :

$$bq' \leqslant a' < b(q' + 1).$$

Si $bq' = a'$, alors $a = b(-q') = bq$ (avec $q = -q'$).
Si $bq' \neq a'$, alors $bq' < a' < b(q' + 1)$,
soit

$$b[-(q' + 1)] < -a' < b(-q')$$

ou encore

$$bq < a < b(q + 1)$$

en posant $q = -(q' + 1)$.
Dans tous les cas, il existe donc un entier relatif q *unique* tel que

(1) $$bq \leqslant a < b(q + 1).$$

Posons $r = a - bq$.

Des inégalités (1), il résulte que :

$$a - bq \geqslant 0, \quad \text{soit} \quad r \geqslant 0,$$

et

$$a - bq < b \quad , \quad \text{soit} \quad r < b.$$

Théorème et définition.

Étant donnés deux entiers relatifs a et $b (b > 0)$, il existe un couple unique (q, r) d'entiers relatifs tels que :

$$a = bq + r \quad \text{et} \quad 0 \leqslant r < b.$$

L'opération permettant de passer du couple (a, b) au couple (q, r) s'appelle *division euclidienne* de a par b. Les nombres q et r sont respectivement le *quotient* et le *reste* dans cette division.

EXEMPLES

1. $a = 513, \quad b = 25.$

$$513 = 25 \times 20 + 13,$$

donc $q = 20$ et $r = 13.$

2. $a = -513 \quad , \quad b = 25.$

$$-513 = 25 \times (-21) + 12,$$

donc $q = -21$ et $r = 12.$

Il est à remarquer sur ces exemples 1 et 2 que deux nombres opposés n'ont pas toujours deux quotients opposés.

3. $a = 436, \quad b = 4.$

$$436 = 4 \times 109,$$

donc $q = 109$ et $r = 0.$

4. $a = -436, \quad b = 4.$

$$-436 = 4 \times (-109),$$

donc $q = -109$ et $r = 0.$

Pour ces deux exemples 3 et 4, les nombres considérés sont opposés, les restes sont nuls, les quotients sont opposés.

2. 6 SOUS-GROUPES DU GROUPE $(\mathbb{Z}, +)$

a) Sous-groupe d'un groupe (G, ⋆).

Définition.

On dit qu'un ensemble E est un sous-groupe d'un groupe (G, ⋆) si et seulement si

i. E est une partie stable de (G, ⋆).

ii. Pour la loi induite sur E par la loi interne de G, (E, ⋆) est un groupe.

Par exemple G est un sous-groupe de lui-même; de même, e étant l'élément neutre de G, $\{e\}$ est un sous-groupe de G. Les sous-groupes de G distincts de G et $\{e\}$ sont appelés **sous-groupes propres** de G.

Nous allons établir une condition nécessaire et suffisante pour qu'un sous-ensemble E de G soit un sous-groupe de (G, ⋆).

Condition nécessaire.

Soit (G, ⋆) un groupe, e son élément neutre. Supposons que (E, ⋆) soit un sous-groupe de G. Soit e_1 l'élément neutre de (E, ⋆), montrons que $e_1 = e$:

dans (G, $\star$) $e \star e_1 = e_1 \star e = e_1$ et dans (E, $\star$) $e_1 \star e_1 = e_1$ donc $e_1 \star e_1 = e \star e_1$ et en simplifiant : $e_1 = e$.
Soit x un élément de E ayant pour symétriques x' et x'_1 respectivement dans (G, $\star$) et (E, $\star$), montrons que $x'_1 = x'$:
dans (G, $\star$) $x \star x' = x' \star x = e$ et dans (E, $\star$) $x \star x'_1 = x'_1 \star x = e_1$. Comme $e_1 = e$, on a $x'_1 \star x = x' \star x$ et en simplifiant : $x'_1 = x'$.
Soit alors x et y quelconques de E, on vient de voir que E comprend y' symétrique de y dans (G, $\star$) donc E comprend $x \star y'$. Donc :

$$[(E, \star) \text{ sous-groupe de } (G, \star)] \Longrightarrow \begin{cases} E \subset G \quad \text{et} \quad E \neq \varnothing \\ \text{et} \\ (\forall (x, y) \in E \times E) \quad x \star y' \in E. \end{cases}$$

Condition suffisante.

Soit E une partie non vide de G telle que

$$(\forall (x, y) \in E \times E) \qquad x \star y' \in E, \qquad y' \text{ étant le symétrique de } y \text{ dans } (G, \star).$$

L'ensemble E comprend au moins un élément x; appliquons la propriété au couple (x, x); nous aurons : $x \star x' \in E$, or $x \star x' = e$, donc $e \in E$.
Étant donné un élément quelconque x de E, appliquons la propriété au couple (e, x). Il vient : $e \star x' \in E$, soit $x' \in E$. Donc, tout élément de E admet un symétrique qui appartient à E. Soit deux éléments quelconques x, y de E. Démontrons que $\star$ est une loi de composition interne dans E. Le symétrique y' de y appartenant à E, on peut appliquer la propriété au couple (x, y'), ce qui donne : $x \star (y')' = x \star y \in E$.
Enfin, puisque $E \subset G$, la loi $\star$ étant associative dans G l'est dans E.
Les axiomes de groupe sont donc vérifiés par (E, $\star$).

Théorème 1.

Une partie E d'un groupe (G, $\star$) est un sous-groupe du groupe G si et seulement si
i. E est une partie non vide.
ii. Quel que soit le couple (x, y) de $E \times E$ on a

$$x \star y' \in E, \qquad y' \text{ étant le symétrique de } y \text{ dans } (G, \star).$$

En notation additive la condition s'écrira

$$x - y \in E,$$

et en notation multiplicative

$$xy^{-1} \in E.$$

EXERCICE 1

E_1 et E_2 étant deux sous-groupes d'un groupe $(G, \star)$ démontrer que $E_1 \cap E_2$ est un sous-groupe de G, $\star$).

b) Multiples d'un entier relatif.

Définition.

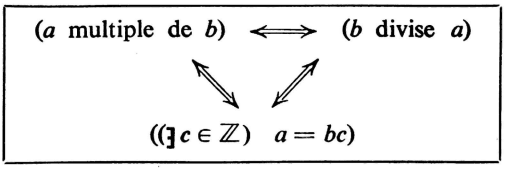
On dit qu'un entier relatif a est un **multiple** d'un entier relatif b si et seulement s'il existe un entier relatif c tel que

$$a = bc.$$

On dit aussi dans ce cas que b **divise** a et l'on écrit

$$b|a.$$

On a donc quels que soient a et b de $\mathbb{Z}$



Si $b > 0$, la relation « a est multiple de b » signifie encore que, dans la *division euclidienne* de a par b, *le reste est nul.*

Remarquons que tous les multiples de 0 sont égaux à 0, donc que 0 divise tout entier relatif.

Remarquons aussi que la relation $(-b)(-c) = bc$ montre que l'ensemble des multiples de b est identique à l'ensemble des multiples de $-b$.

Notation. Nous noterons $n\mathbb{Z}$ l'ensemble des multiples de l'entier relatif n.

Comme nous venons de le voir $(-n)\ \mathbb{Z} = n\mathbb{Z}$. **Nous pouvons donc supposer $n \geqslant 0$.** L'entier naturel n étant fixé, $n\mathbb{Z}$ est une partie de $\mathbb{Z}$, elle est non vide car $0 \in n\mathbb{Z}$. Soit deux éléments quelconques x et x' de $n\mathbb{Z}$; il existe q et q' de $\mathbb{Z}$ tels que

$$x = qn \quad , \quad x' = q'n.$$

On a donc

$$x - x' = (q - q')\, n;$$

or $q - q' \in \mathbb{Z}$, donc $x - x' \in \mathbb{Z}$; par conséquent (cf. théorème 1) $n\mathbb{Z}$ est un sous-groupe du groupe $(\mathbb{Z}, +)$. Nous allons montrer que *tout* sous-groupe de $(\mathbb{Z}, +)$ est de cette forme.

c) Sous-groupes du groupe $(\mathbb{Z}, +)$.

Soit E un sous-groupe de $(\mathbb{Z}, +)$.

Si $E = \{0\}$, on peut écrire $E = 0\,\mathbb{Z}$.

Si $E \neq \{0\}$, E contient au moins un élément $x_0 \neq 0$, et son opposé $(-x_0)$; l'un de ces deux nombres est strictement positif. E contient donc des entiers strictement positifs. Soit n *le plus petit élément strictement positif de* E.

Tout multiple de n appartient à E. En effet :

si $k = 0$, $nk = 0 \in E$.

si $k > 0$, nk est la somme de k termes égaux à n et, puisque l'addition est une loi de composition interne dans E, $nk \in E$.

si $k < 0$, $-k > 0$, d'où $n(-k) \in E$ et $-[n(-k)] = nk \in E$.

Concluons : $n\mathbb{Z} \subset E$.

Inversement, soit x un élément quelconque de $(E, +)$. On peut effectuer la division euclidienne de x par n. On obtient :

$$x = nq + r \quad \text{et} \quad 0 \leqslant r < n.$$

Les entiers x et n appartiennent à E ; E étant un sous-groupe de $\mathbb{Z}$, E comprend x et nq donc $x - nq = r$ (cf. théorème 1).

Il est impossible que $r \neq 0$; car on aurait $0 < r < n$ et n ne serait pas le plus petit élément strictement positif de E. Donc $r = 0$ et tout élément x de E est un multiple de n, c'est-à-dire $E \subset n\mathbb{Z}$.

Il en résulte que

$$E = n\mathbb{Z}.$$

Dans cette étude nous avons supposé $n > 0$. Pour $n = 0$ on retrouve le sous-groupe $\{0\}$. Remarquons que pour $n = 1$ on trouve le sous-groupe $\mathbb{Z}$ lui-même. Concluons.

Théorème 2.

Tout sous-groupe de $(\mathbb{Z}, +)$ est de la forme $n\mathbb{Z}$ où n est un entier naturel quelconque.

Rappelons que si $n > 0$ alors n est le *plus petit entier strictement positif* du sous-groupe $n\mathbb{Z}$. Donc si $n\mathbb{Z} = n'\mathbb{Z}$ $(n, n' \in \mathbb{N})$ on a $n = n'$; on pourrait aussi supposer $n \in \mathbb{Z}$, dans ce cas, si $n\mathbb{Z} = n'\mathbb{Z}$ $(n, n' \in \mathbb{Z})$, on aurait $n = n'$ ou $n = -n'$.

EXERCICE

Soit $E = \{x \in \mathbb{Z} \mid \exists (a, b) \in \mathbb{Z} \times \mathbb{Z} \quad x = 5a + 15b\}$.
Démontrer que E est un sous-groupe de $\mathbb{Z}$, ensemble des multiples d'un entier que l'on précisera.

2. 7 SOUS-ANNEAUX ET IDÉAUX DE L'ANNEAU $(\mathbb{Z}, +, \times)$

a) Notion de sous-anneau. Sous-anneaux de $(\mathbb{Z}, +, \times)$.

Définition.

On dit qu'un ensemble B est un sous-anneau d'un anneau $(A, +, \times)$ si et seulement si
i. B est une partie stable de A pour l'addition et la multiplication.
ii. Pour les lois induites sur B par les lois internes de A, $(B, +, \times)$ est un anneau.

Par exemple tout anneau A est sous-anneau de lui-même; de même $\{0_A\}$ est un sous-anneau de l'anneau A. Tout sous-anneau de A distinct de $\{0_A\}$ et de A est appelé **sous-anneau propre** de A.

EXERCICES

1. Démontrer qu'une partie B d'un anneau $(A, +, \times)$ est un sous-anneau de A si et seulement si
   i. B est non vide.
   ii. $(\forall (x, y) \in B \times B) \quad x - y \in B$.
   iii. $(\forall (x, y) \in B \times B) \quad xy \in B$.
   On voit donc qu'un sous-anneau B de l'anneau A est un *sous-groupe* de $(A, +)$ qui, de plus, est stable pour la multiplication de l'anneau.
2. Démontrer que l'intersection de deux sous-anneaux de A est encore un sous-anneau de A.

Les sous-anneaux de l'anneau A sont donc à chercher parmi les sous-groupes du groupe $(A, +)$.
Par conséquent les sous-anneaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ $(n \in \mathbb{Z})$. Comme le produit de deux multiples entiers de n, c'est-à-dire de deux éléments de $n\mathbb{Z}$, est encore un élément de $n\mathbb{Z}$, quel que soit l'entier naturel n, nous pouvons énoncer.

Théorème.

Tout sous-anneau de l'anneau $\mathbb{Z}$ est de la forme $n\mathbb{Z}$ où n est un entier naturel quelconque.

Pour $n = 0$ on trouve $\{0\}$ et pour $n = 1$, $\mathbb{Z}$, c'est-à-dire les deux sous-anneaux triviaux de l'anneau $\mathbb{Z}$.

REMARQUE 1

Dans le cas de $\mathbb{Z}$ les sous-groupes de $(\mathbb{Z}, +)$ et les sous-anneaux de $(\mathbb{Z}, +, \times)$ sont identiques. C'est un cas particulier comme le montrent les exercices suivants.

EXERCICES

3. On munit l'ensemble $F = \mathcal{F}(\mathbb{R}, \mathbb{R})$ des fonctions numériques sur $\mathbb{R}$ de l'addition $(f, g) \longmapsto s = f + g$ et de la multiplication $(f, g) \longmapsto p = fg$ suivantes
$$(\forall x \in \mathbb{R}) \quad s(x) = f(x) + g(x) \quad \text{et} \quad p(x) = f(x)\,g(x).$$
Démontrer que $(F, +, \times)$ est un anneau commutatif unitaire. Quels sont les éléments neutres de l'addition et de la multiplication?

4. On désigne par $P = \mathcal{P}(\mathbb{R}, \mathbb{R})$ l'ensemble des fonctions polynômes à coefficients et variable réels et par P_n l'ensemble de ces polynômes de degré $\leqslant n$.
Démontrer que P est à la fois sous-groupe de $(F, +)$ et sous-anneau de $(F, +, \times)$ (cf. exercice 3 ci-dessus).
Démontrer que P_n est un sous-groupe de $(F, +)$ et de $(P, +)$.
P_n est-il un sous-anneau de $(F, +, \times)$? de $(P, +, \times)$?

b) Notion d'idéal d'un anneau commutatif. Idéaux de $(\mathbb{Z}, +, \times)$.

Définition.

Étant donné un anneau *commutatif* $(A, +, \times)$ on appelle **idéal** de A toute partie *non vide* I de A telle que

(1) $\quad (\forall (x, y) \in I \times I) \quad x - y \in I,$

(2) $\quad (\forall x \in I)\ (\forall z \in A) \quad xz \in I.$

On voit immédiatement que $\{0_A\}$ et A sont des idéaux de l'anneau commutatif A. Tout idéal distinct de $\{0_A\}$ et A est appelé **idéal propre** de l'anneau A.
La propriété (1) montre que tout idéal I de l'anneau commutatif A est un sous-groupe du groupe $(A, +)$.
Si l'anneau A a un élément unité e on voit immédiatement en utilisant la propriété (2) que tout idéal I de A contenant e est égal à A tout entier. En effet $e \in I$ et (2) entraînent que

$$(\forall z \in A) \qquad ez = z \in I;$$

donc $I = A$.

EXEMPLE

Dans l'anneau $(\mathbb{Z}, +, \times)$, considérons le sous-ensemble $3\,\mathbb{Z}$. Nous savons déjà que c'est un sous-groupe de $(\mathbb{Z}, +)$. Vérifions la propriété (2).
Soit $x \in 3\,\mathbb{Z}$. Cela signifie qu'il existe un nombre $k \in \mathbb{Z}$ tel que $x = 3k$. Soit z entier relatif quelconque on a

$$\begin{aligned} xz &= (3k)\,z \\ &= 3\,(kz) \end{aligned}$$

or $kz \in \mathbb{Z}$ donc $xz \in 3\,\mathbb{Z}$.
Nous pouvons en déduire que (2) est vérifiée quel que soit $x \in 3\,\mathbb{Z}$ et quel que soit $z \in \mathbb{Z}$.
Le sous-groupe $(3\,\mathbb{Z}, +)$ de $(\mathbb{Z}, +)$ est donc un *idéal* de $(\mathbb{Z}, +, \times)$.

EXERCICES

5. Soit $I = \{z \in \mathbb{Z} \mid (\exists (u, v) \in \mathbb{Z} \times \mathbb{Z}) \quad z = ua + vb\}$, où a et b sont deux entiers relatifs donnés. Démontrer que I est un idéal de $(\mathbb{Z}, +, \times)$.

6. Soit I_1 et I_2 deux idéaux d'un anneau commutatif $(A, +, \times)$. Démontrer que $I_1 \cap I_2$ est un idéal de A.

Cherchons les idéaux de $(\mathbb{Z}, +, \times)$. Soit I un idéal quelconque de $\mathbb{Z}$. L'ensemble I est donc non vide, vérifie la propriété (1) : c'est donc un sous-groupe additif de $\mathbb{Z}$; il est donc de la forme $n\mathbb{Z}$ (cf. § 2.6 *c*). Inversement, il est aisé de vérifier, comme nous l'avons fait pour $n = 3$, que les sous-ensembles $n\mathbb{Z}$ de $\mathbb{Z}$ sont des idéaux de $(\mathbb{Z}, +, \times)$.

Théorème.

Tout idéal I de l'anneau $(\mathbb{Z}, +, \times)$ est de la forme $n\mathbb{Z}$ où n est un entier naturel quelconque.

Rappelons que si $n > 0$ l'entier naturel n est le plus petit élément strictement positif de $n\mathbb{Z}$.

L'idéal $1.\mathbb{Z}$ est égal à $\mathbb{Z}$.

Tout idéal qui contient 1 est égal à $\mathbb{Z}$, puisque le plus petit élément strictement positif de cet idéal ne peut être que 1 : nous retrouvons pour l'anneau $\mathbb{Z}$ la propriété donnée plus haut pour tout idéal I de A contenant l'élément unité de A.

REMARQUE 2

Soit A un anneau commutatif quelconque et I un idéal de A ; la propriété (2) entraîne la propriété (2′) (car $I \subset A$)

(2′) $\qquad (\forall (x,\ z) \in I \times I) \qquad xz \in I$;

donc I est non vide, vérifie (1) et (2′) ; par conséquent tout *idéal* de A est un *sous-anneau* de A.

Dans le cas de l'anneau $\mathbb{Z}$ nous avons trouvé que les idéaux de $\mathbb{Z}$ étaient identiques aux sous-anneaux de $\mathbb{Z}$: c'est un cas particulier. Voici un contre-exemple : vous avez étudié dans les classes précédentes le corps commutatif $\mathbb{Q}$ des nombres rationnels ; l'addition et la multiplication de $\mathbb{Q}$ possèdent toutes les propriétés de ces opérations dans un anneau commutatif (avec en plus l'inversibilité de tout rationnel non nul, propriété qui ne nous intéresse pas ici). Or il est évident que $\mathbb{Z}$ est un sous-anneau de $\mathbb{Q}$, considéré comme anneau commutatif. En revanche $\mathbb{Z}$ n'est pas un idéal de $\mathbb{Q}$, considéré comme anneau commutatif, car le produit d'un entier quelconque par un rationnel quelconque n'est pas forcément un entier.

EXERCICE

7. On reprend les notations des exercices 3 et 4 ci-dessus ; P, sous-anneau de $(F, +, \times)$, est-il un idéal de l'anneau commutatif F ?
(Considérer $f \in P$ et $g \in F$ définies quel que soit $x \in \mathbb{R}$ par

$$f(x) = x + 1 \quad \text{et} \quad g(x) = \frac{1}{x^2 + 1}\Big).$$

2. 8 ENSEMBLE $\mathbb{Z}/n\mathbb{Z}$ DES ENTIERS MODULO n

a) Congruences modulo n.

Considérons, l'entier naturel n étant donné, la relation binaire $\mathcal{R}$ définie quels que soient x et y de $\mathbb{Z}$ par

$$x - y \in n\mathbb{Z}.$$

Cette relation est *réflexive* car, quel que soit x de $\mathbb{Z}$, on a

$$x - x = 0 \in n\mathbb{Z}.$$

D'autre part elle est *symétrique* car, $n\mathbb{Z}$ étant un groupe si $x - y \in n\mathbb{Z}$, alors $y - x = -(x - y) \in n\mathbb{Z}$ et ceci quels que soient x et y de $\mathbb{Z}$.

Enfin elle est *transitive* car, l'addition étant une loi interne définie sur $n\mathbb{Z}$, si $x - y$ et $y - z$ sont des éléments de $n\mathbb{Z}$ alors $(x - y) + (y - z) = x - z$ est un élément de $n\mathbb{Z}$ et ceci quel que soit x, y, z de $\mathbb{Z}$. Concluons.

Théorème et définition.

Étant donné un entier naturel n la relation binaire définie quels que soient x et y de $\mathbb{Z}$ par

$$x - y \in n\mathbb{Z}$$

est une relation d'équivalence dans $\mathbb{Z}$. On l'appelle **congruence modulo** n et on la note

$$x \equiv y \pmod{n}$$

La relation $x \equiv y \pmod{n}$ peut se lire « x est congru à y, modulo n ». Si $n = 0$, cette relation devient $x - y \in \{0\}$, c'est l'*égalité* $x = y$, relation d'équivalence triviale; dans ce cas chaque classe d'équivalence comprend un seul représentant.

Si $n > 0$ nous allons voir que, quels que soient x et y de $\mathbb{Z}$ on a

$(x \equiv y \pmod{n}) \iff$ (x et y ont même reste dans la division euclidienne par n)

Supposons $x \equiv y \pmod{n}$. Alors, il existe un nombre entier relatif k tel que $x = y + kn$. La division euclidienne de y par n donne :

$$y = nq + r \quad \text{et} \quad 0 \leqslant r < n,$$

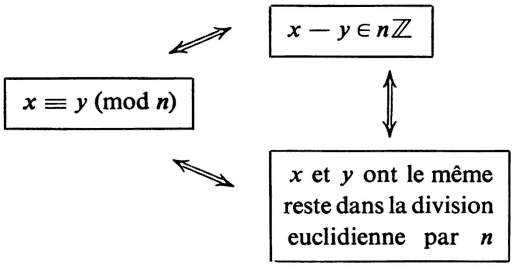
d'où : $x = n(q + k) + r$ et $0 \leqslant r < n$.
Les deux nombres x et y ont donc le même reste r dans la division par n.

Réciproquement, supposons que x et y admettent le même reste dans la division par n.

On peut donc écrire :

$$\begin{aligned} x &= nq + r \\ y &= nq' + r \end{aligned} \quad \text{et} \quad 0 \leqslant r < n,$$

d'où : $x - y = n(q - q')$, et par suite $x \equiv y \pmod{n}$.
En résumé si $n > 0$ quels que soient x et y de $\mathbb{Z}$ on a



b) Ensemble des entiers modulo n.

La relation $\mathcal{R}$, congruence modulo n, s'écrivant $x - y \in n\mathbb{Z}$, au lieu de noter l'ensemble quotient $\mathbb{Z}/\mathcal{R}$ on l'écrit $\mathbb{Z}/n\mathbb{Z}$.
Les classes d'équivalence pour la congruence modulo n, c'est-à-dire les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont appelées *classes résiduelles modulo n* ou plus simplement **entiers modulo n.**
Étudions ces classes.
Pour $n = 0$, la classe de x, soit $\dot{x}$, contient un seul élément x, puisque la congruence modulo 0 est l'égalité.

Pour $n > 0$, la classe de x, notée $\dot{x}$, contient tous les éléments de $\mathbb{Z}$ équivalents à x, c'est-à-dire tous les entiers relatifs qui admettent même reste que x dans la division par n.

On en déduit immédiatement qu'il y a autant d'éléments dans $\mathbb{Z}/n\mathbb{Z}$ que de restes possibles dans la division par n, c'est-à-dire n puisque $0 \leqslant r < n$. On les note

$\dot{0}, \dot{1}, \dot{2}, \ldots, \widehat{\dot{n-1}}$.

EXEMPLE

$\mathbb{Z}/3\,\mathbb{Z}$ contient 3 éléments :

$\dot{0} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\} = 3\,\mathbb{Z}$,
$\dot{1} = \{\ldots, -8, -5, -2, +1, +4, +7, \ldots\}$,
$\dot{2} = \{\ldots, -7, -4, -1, +2, +5, \ldots\}$.

REMARQUE

Lorsque nous considérons une *seule congruence modulo n* nous noterons ses classes $\dot{0}, \dot{1}, \ldots, \widehat{(\dot{n-1})}$ et ceci quel que soit n.

En revanche si nous considérons *simultanément* plusieurs congruences, modulo n, modulo $n' \neq n$... il faudra utiliser des notations différentes pour les entiers modulo n et pour les entiers modulo n'.

Prenons $n = 3$ et $n' = 8$ nous pourrons poser

$$\mathbb{Z}/3\,\mathbb{Z} = \{\dot{0}, \dot{1}, \dot{2}\},$$
$$\mathbb{Z}/8\,\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}.$$

On voit que l'on a, par exemple,

$$\dot{2} = \{\ldots, -7, -4, -1, 2, 5 \ldots\} \neq \{\ldots, -14, -6, 2, 10, 18 \ldots\} = \bar{2}.$$

Prendre la même notation dans un même calcul pour la classe de 2 modulo 3 et pour la classe de 2 modulo 8 entraînerait de lourdes erreurs.

2. 9 ADDITION ET MULTIPLICATION DANS $\mathbb{Z}/n\mathbb{Z}$

Nous connaissons un entier modulo n, $\dot{x}$, par ses représentants $x, x+n, x+2n \ldots, x-n, x-2n \ldots$; nous allons essayer de définir une addition et une multiplication dans $\mathbb{Z}/n\mathbb{Z}$ en utilisant l'addition et la multiplication dans $\mathbb{Z}$; l'exemple suivant montre qu'il faut être très prudent.

a) Introduction. Étude d'un exemple.

Nous avons vu en Seconde que l'on appelle fraction d'entiers relatifs tout couple (a, a') élément de $\mathbb{Z} \times \mathbb{Z}^*$, cette fraction se note $\frac{a}{a'}$. Dans l'ensemble $\mathcal{F}$ des fractions vous avez vu que la relation $aa'_1 = a'a_1$ entre les fractions $\frac{a}{a'}$ et $\frac{a_1}{a'_1}$ est une relation d'équivalence et qu'un nombre rationnel α est une classe d'équivalence de fractions pour cette relation d'équivalence. L'ensemble des nombres rationnels est l'ensemble $\mathbb{Q}$.

Soit α et β deux nombres rationnels de représentants respectifs $\frac{a}{a'}$ et $\frac{b}{b'}$; pouvons-nous définir une loi interne $\star$ sur $\mathbb{Q}$ en disant $\alpha \star \beta$ a pour représentant $\frac{a+b}{a'+b'}$?

Prenons α ayant pour représentants $\frac{2}{3}, \frac{4}{6} \ldots$

— β — $\frac{1}{5}, \frac{3}{15}, \ldots$

Le rationnel $\alpha \star \beta$, s'il existait, aurait pour représentants

$$\frac{2+1}{3+5} = \frac{3}{8} \quad , \quad \frac{4+3}{6+15} = \frac{7}{21} \cdots$$

Or ces fractions ne définissent pas le même rationnel; il est donc impossible de définire une loi interne par le procédé indiqué.

En revanche en associant à α et β le rationnel de représentant $\frac{ab}{a'b'}$ on voit que, quels que soient les représentants choisis pour α et β, les fractions obtenues sont équivalentes Avec le même exemple que ci-dessus on a

tous les représentants de α sont de la forme $\frac{2k}{3k}$,

— β — $\frac{1h}{5h}$,

où k et h sont des entiers relatifs quelconques. Toutes les fractions $\frac{(2k)(1h)}{(3k)(5h)}$ sont équivalentes, elles représentent le même rationnel qui, comme vous le savez, est le produit $\alpha\beta$. Cet exemple va nous conduire à une notion importante.

b) Compatibilité entre une relation d'équivalence et une loi interne définies sur le même ensemble.

Soit E un ensemble *muni à la fois*

1) d'une relation d'équivalence notée

$$x \equiv x' \pmod{\mathcal{R}}$$

2) d'une loi interne

$$(x, y) \longmapsto x \mathrm{T} y.$$

On dit que la relation d'équivalence $\mathcal{R}$ et la loi interne T sont **compatibles** si et seulement si,
quels que soient x, x', y, y' de E, on a

$$\left\{ \begin{array}{l} x \equiv x' \pmod{\mathcal{R}} \\ \quad \text{et} \\ y \equiv y' \pmod{\mathcal{R}} \end{array} \right. \Longrightarrow [x \mathrm{T} y \equiv x' \mathrm{T} y' \pmod{\mathcal{R}}]$$

Dans l'ensemble $\mathcal{F}$ des fractions la loi interne

$$\left(\frac{a}{a'}, \frac{b}{b'}\right) \longmapsto \frac{a+b}{a'+b'}$$

n'est pas compatible avec l'équivalence des fractions.
En revanche la loi interne

$$\left(\frac{a}{a'}, \frac{b}{b'}\right) \longmapsto \frac{aa'}{bb'}$$

est compatible avec l'équivalence des fractions.

Si la relation d'équivalence $\mathcal{R}$ et la loi interne T définies toutes deux sur E sont compatibles, quels que soient les représentants respectifs x' et y' de $\dot{x}$ et $\dot{y}$, éléments de $E/\mathcal{R}$, les éléments $x' \mathrm{T} y'$ de E sont *tous équivalents entre eux*, modulo $\mathcal{R}$; ce sont les représentants d'un élément parfaitement déterminé de $E/\mathcal{R}$. Nous définissons ainsi à partir d'un couple $(\dot{x}, \dot{y}) \in E/\mathcal{R} \times E/\mathcal{R}$ un élément unique de $E/\mathcal{R}$, c'est-à-dire une loi interne sur $E/\mathcal{R}$.
Cette loi interne sur $E/\mathcal{R}$ est associée à la loi interne T sur E, on l'appelle **loi quotient** de la loi T par la relation d'équivalence $\mathcal{R}$ on la note en général $\dot{\mathrm{T}}$.

Par conséquent, la relation d'équivalence $\mathcal{R}$ et la loi interne T *toutes deux définies sur E étant compatibles*, on posera **par définition** quels que soient les représentants respectifs x' et y' de $\dot{x}$ et $\dot{y}$

$$\dot{x}\,\dot{\mathsf{T}}\,\dot{y} = \widehat{x'\,\mathsf{T}\,y'};$$

comme x et y sont par définition des représentants de $\dot{x}$ et $\dot{y}$ on écrira plus simplement

$$\dot{x}\,\dot{\mathsf{T}}\,\dot{y} = \widehat{x\,\mathsf{T}\,y}.$$

c) Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

Il est très simple de vérifier que l'addition et la multiplication dans $\mathbb{Z}$ sont compatibles avec la relation de congruence modulo n. En effet, si on a

$$x \equiv x' \pmod{n} \quad \text{et} \quad y \equiv y' \pmod{n}$$

il existe h et k de $\mathbb{Z}$ tels que

$$x = x' + kn \quad \text{et} \quad y = y' + hn,$$

d'où on déduit

$$x + y = x' + kn + y' + hn = (x' + y') + (k + h)\,n$$
$$xy = (x' + kn)(y' + hn) = x'y' + (x'h + y'k + hkn)\,n;$$

comme $k + h$ et $x'h + y'k + hkn$ sont des entiers, on voit que l'on a quels que soient x, x', y, y' de $\mathbb{Z}$

$$\begin{cases} x \equiv x' \pmod{n} \\ \text{et} \\ y \equiv y' \pmod{n} \end{cases} \Longrightarrow \begin{cases} x + y \equiv x' + y' \pmod{n} \\ \text{et} \\ xy \equiv x'y' \pmod{n} \end{cases}$$

Théorème.

L'addition et la multiplication définies sur $\mathbb{Z}$ sont compatibles avec la relation d'équivalence définie sur $\mathbb{Z}$ appelée congruence modulo n.

Quelles que soient les classes $\dot{x}$ et $\dot{y}$ éléments de $\mathbb{Z}/n\mathbb{Z}$ nous **définissons** dans $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication notées provisoirement $\dot{+}$ et $\dot{\times}$ en posant quels que soient les entiers modulo n, $\dot{x}$ et $\dot{y}$

$$\boxed{\dot{x} \dot{+} \dot{y} = \widehat{(x + y)} \quad , \quad \dot{x} \dot{\times} \dot{y} = \widehat{xy}.}$$

Les lois internes $\dot{+}$ et $\dot{\times}$ définies sur $\mathbb{Z}/n\mathbb{Z}$ sont les lois quotients respectivement de l'addition et de la multiplication sur $\mathbb{Z}$ par la relation d'équivalence congruence modulo n.

EXERCICE 1

Construire les tables d'addition et de multiplication de $\mathbb{Z}/5\,\mathbb{Z}$ et de $\mathbb{Z}/6\,\mathbb{Z}$.

REMARQUE

La compatibilité de l'addition et de la multiplication avec la relation de congruence modulo n peut encore s'exprimer ainsi :
En ajoutant ou en multipliant membre à membre deux congruences modulo n, on obtient encore des congruences modulo n.

Les propriétés de l'addition et de la multiplication dans $\mathbb{Z}$ et les formules — encadrées plus haut — définissant l'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ vont nous donner les propriétés de ces dernières.

d) Groupe $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$.

Soit trois entiers modulo n quelconques $\dot{x}$, $\dot{y}$, $\dot{z}$; nous avons

$$\begin{aligned}
\dot{x} \dot{+} (\dot{y} \dot{+} \dot{z}) &= \dot{x} \dot{+} \widehat{(y + z)} = \widehat{x + (y + z)}, && \text{(définition de } \dot{+}) \\
&= \widehat{(x + y) + z}, && \text{(associativité de } + \text{ dans } \mathbb{Z}) \\
&= \widehat{(x + y)} \dot{+} \dot{z} = (\dot{x} \dot{+} \dot{y}) \dot{+} \dot{z}; && \text{(définition de } \dot{+})
\end{aligned}$$

l'addition dans $\mathbb{Z}/n\mathbb{Z}$ est donc *associative*.
Soit deux entiers modulo n quelconques $\dot{x}$, $\dot{y}$; nous avons

$$\begin{aligned}
\dot{x} \dot{+} \dot{y} &= \widehat{x + y}, && \text{(définition de } \dot{+}) \\
&= \widehat{y + x}, && \text{(commutativité de } + \text{ dans } \mathbb{Z}) \\
&= \dot{y} \dot{+} \dot{x}; && \text{(définition de } \dot{+})
\end{aligned}$$

l'addition dans $\mathbb{Z}/n\mathbb{Z}$ est donc *commutative*.
Quel que soit l'élément $\dot{x}$ de $\mathbb{Z}/n\mathbb{Z}$ on a

$$\begin{aligned}
\dot{0} \dot{+} \dot{x} &= \widehat{0 + x}, && \text{(définition de } \dot{+}) \\
&= \dot{x}; && \text{(0 élément neutre dans } \mathbb{Z}) \\
\dot{x} \dot{+} \widehat{(-x)} &= \widehat{x + (-x)}, && \text{(définition de } \dot{+}) \\
&= \dot{0}. && (x \text{ et } -x \text{ sont opposés dans } \mathbb{Z})
\end{aligned}$$

On montrerait de même que $\dot{x} \dot{+} \dot{0} = \dot{x}$ et $\widehat{(-x)} \dot{+} \dot{x} = \dot{0}$ donc l'addition dans $\mathbb{Z}/n\mathbb{Z}$ a un *élément neutre* $\dot{0}$ *et tout élément* $\dot{x}$ *a un opposé* $\widehat{(-x)}$ que nous noterons aussi $-(\dot{x})$.
Concluons

Théorème.

$(\mathbb{Z}/n\mathbb{Z}, \dot{+})$ est un groupe commutatif.

e) Anneau $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$

On démontre exactement comme pour l'addition — faites-le à titre d'exercice — que la *multiplication* dans $\mathbb{Z}/n\mathbb{Z}$ est *associative*, *commutative* et qu'elle possède un *élément neutre* $\dot{1}$.

Soit enfin trois entiers modulo n quelconques $\dot{x}$, $\dot{y}$ et $\dot{z}$ on a

$$\begin{aligned}
\dot{x} \dot{\times} (\dot{y} \dot{+} \dot{z}) &= \dot{x} \dot{\times} \widehat{(y + z)}, && \text{(définition de } \dot{+}) \\
&= \widehat{x \times (y + z)}, && \text{(définition de } \dot{\times}) \\
&= \widehat{(x \times y) + (x \times z)}, && \text{(distributivité dans } \mathbb{Z}) \\
&= \widehat{(x \times y)} \dot{+} \widehat{(x \times z)}, && \text{(définition de } \dot{+}) \\
&= (\dot{x} \dot{\times} \dot{y}) \dot{+} (\dot{x} \dot{\times} \dot{z}); && \text{(définition de } \dot{\times})
\end{aligned}$$

la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ est donc distributive par rapport à l'addition. Concluons :

Théorème.

$(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$ est un anneau commutatif unitaire.

f) Cas particuliers.

ATTENTION! Il ne faudrait pas généraliser inconsidérément les résultats démontrés ci-dessus et croire que toutes les propriétés de $\mathbb{Z}$ sont vraies pour $\mathbb{Z}/n\mathbb{Z}$. Voici deux contre-exemples.

1. Dans $\mathbb{Z}/6\,\mathbb{Z}$ il y a des diviseurs de zéro par exemple

$$\dot{2} \neq \dot{0} \quad , \quad \dot{3} \neq \dot{0} \quad , \quad \dot{2} \dot{\times} \dot{3} = \dot{6} = \dot{0}.$$

De même si $n = pq$, avec $1 < p < n$ on a $\dot{p} \dot{\times} \dot{q} = \widehat{p \times q} = \dot{n} = \dot{0}$ avec $\dot{p} \neq \dot{0}$ et $\dot{q} \neq \dot{0}$. Concluons

Si $n = pq$ avec $1 < p < n$, l'anneau $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de zéro.

2. Dans $\mathbb{Z}/5\,\mathbb{Z}$ on a

$$\dot{1} \dot{\times} \dot{1} = \dot{1} \quad , \quad \dot{2} \dot{\times} \dot{3} = \dot{6} = \dot{1} \quad , \quad \dot{4} \dot{\times} \dot{4} = \dot{16} = \dot{1}.$$

Donc dans $\mathbb{Z}/5\,\mathbb{Z}$ tout élément distinct de $\dot{0}$ est inversible alors que dans $\mathbb{Z}$ seuls 1 et -1 sont inversibles (cf. § 2.3 *c*). Nous reviendrons sur cet exemple au § 2.11.

Auparavant, dans le § 2.10, revenant au cas général nous allons dégager la notion d'homomorphisme.

2. 10 HOMOMORPHISMES

a) Introduction.

Considérons toutes les applications de l'ensemble $\mathbb{Z}$ des entiers relatifs dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulo n. Chacune d'elle associe à tout entier relatif un entier modulo n bien déterminé, c'est-à-dire une classe bien déterminée pour la relation de congruence modulo n.
Parmi toutes ces applications, une attire particulièrement l'attention : c'est celle qui associe à tout x de $\mathbb{Z}$ la classe $\dot{x}$ qui contient x. Si nous la désignons par f nous aurons

$$\begin{array}{rccc} f: & \mathbb{Z} & \longmapsto & \mathbb{Z}/n\mathbb{Z} \\ & x & \longmapsto & \dot{x} \end{array}$$

Un élément quelconque de $\mathbb{Z}/n\mathbb{Z}$ est une classe d'équivalence modulo n, elle contient donc au moins un élément $x \in \mathbb{Z}$ dont elle est l'image par f; donc f est *surjective*. Se distinguant de façon naturelle de toutes les autres applications de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ l'application f définie pour tout x de Z par

$$f(x) = \dot{x}$$

est appelée **application canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$.**

EXERCICE 1

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. Comment définirez-vous l'application canonique de E sur $E/\mathcal{R}$?
Dans quel unique cas cette application est-elle injective?

D'autre part, dans le cas qui nous occupe, $\mathbb{Z}$ est muni d'une addition et d'une multiplication ainsi que $\mathbb{Z}/n\mathbb{Z}$. Les formules encadrées données au § 2.9 c nous donnent les schémas suivants quels que soient x et y de $\mathbb{Z}$ (fig. 1)

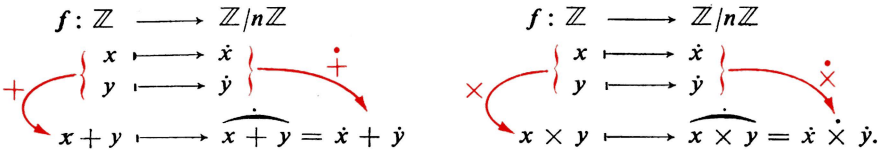


fig.1

Or $\dot{x} = f(x)$, $\dot{y} = f(y)$, $\dot{x+y} = f(x+y)$, $\dot{x \times y} = f(x \times y)$; donc, quels que soient x et y de $\mathbb{Z}$, on a

$$f(x+y) = f(x) \dot{+} f(y) \quad , \quad f(x \times y) = f(x) \dot{\times} f(y).$$

Ceci nous conduit à la définition générale donnée ci-dessous.

b) Notion d'homomorphisme.

Définition.

Étant donnés un ensemble E muni d'une loi interne notée T et un ensemble E′ muni d'une loi interne notée T′, on dit qu'une application f de E dans E′ est un **homomorphisme** de (E, T) dans (E′, T′) si et seulement si

$$(\forall\, (x, y) \in E \times E) \qquad f(x\, T\, y) = f(x)\, T'\, f(y).$$

Si on pose $x' = f(x)$, $y' = f(y)$, on aura

$$\begin{array}{rcl} f: & E & \longrightarrow E' \\ & x & \longmapsto x' \\ & y & \longmapsto y' \\ & x\, T\, y & \longmapsto x'\, T'\, y' \end{array}$$

Autrement dit : l'*image par f du composé* de deux éléments x, y de E pour la loi de E est le *composé des images* x' et y' par f pour la loi de E′.

EXEMPLES

1. L'application canonique f de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est :
   - un homomorphisme surjectif de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, \dot{+})$,
   - — — $(\mathbb{Z}, \times)$ sur $(\mathbb{Z}/n\mathbb{Z}, \dot{\times})$.

   Nous dirons également que f est un homomorphisme surjectif de $(\mathbb{Z}, +, \times)$ sur $(\mathbb{Z}/n\mathbb{Z}, \dot{+}, \dot{\times})$.

2. Considérons $\mathcal{V}_3$ espace vectoriel de dimension 3 sur $\mathcal{R}$ de base $(\vec{i}, \vec{j}, \vec{k})$; soit p la projection de $\mathcal{V}_3$ sur $\mathcal{V}_1$ parallèlement au plan vectoriel $\Pi\,(\vec{j}, \vec{k})$ qui à tout vecteur $\vec{V} = x\vec{i} + y\vec{j} + z\vec{k}$ de $\mathcal{V}_3$ associe le vecteur $\vec{V}' = x\vec{i}$ de $\mathcal{V}_1$.

   Quels que soient les vecteurs $\vec{V}$ et $\vec{W}$ de $\mathcal{V}_3$ on a

$$p(\vec{V} + \vec{W}) = p(\vec{V}) + p(\vec{W})$$

Donc p est un homomorphisme de $(\mathfrak{U}_3, +)$ sur $(\mathfrak{U}_1, +)$. On voit immédiatement que p est surjectif.

3. On considère l'application

$$\begin{array}{rccc} f: & \mathbb{N} & \longrightarrow & \mathbb{N} \\ & n & \longmapsto & 2^n \end{array}$$

Quels que soient n et p de $\mathbb{N}$ on a

$$f(n+p) = 2^{n+p} = 2^n \times 2^p = f(n) \times f(p)$$

Donc f est un homomorphisme de $(\mathbb{N}, +)$ dans $(\mathbb{N}, \times)$. On voit que cet homomorphisme est injectif et non surjectif.

Nous avons conservé jusqu'à maintenant les notations $\dot{+}$ et $\dot{\times}$ pour l'addition et la multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour bien marquer dans les homomorphismes les lois définies sur $\mathbb{Z}$ et celles définies sur $\mathbb{Z}/n\mathbb{Z}$.
Désormais, aucune ambiguïté ne pouvant en résulter, **nous noterons simplement** $\dot{x} + \dot{y}$ la somme de $\dot{x}$ et de $\dot{y}$ et $\dot{x}\dot{y}$ leur produit.

c) Exercices résolus : Propriétés des homomorphismes

Considérons les ensembles E, E′, E″ munis respectivement des lois internes notées T, T′, T″, un homomorphisme f de (E, T) dans (E′, T′) et un homomorphisme g de (E′, T′) dans (E″, T″) nous allons démontrer le théorème suivant :

Théorème 1.

Le composé de deux homomorphismes est un homomorphisme.

Nous avons donc

$$\mathrm{E} \xrightarrow{f} \mathrm{E}' \xrightarrow{g} \mathrm{E}''$$

avec

$$(\forall\, (x, y) \in \mathrm{E} \times \mathrm{E}) \qquad f(x\ \mathrm{T}\ y) = f(x)\ \mathrm{T}'\ f(y),$$

et

$$(\forall\, (x', y') \in \mathrm{E}' \times \mathrm{E}') \qquad g(x'\ \mathrm{T}'\ y') = g(x')\ \mathrm{T}''\ g(y').$$

Nous allons montrer que $g \circ f$ est un homomorphisme de (E, T) dans (E″, T″). En effet, quels que soient x et y de E, nous avons

$$\begin{array}{ll} (g \circ f)(x\ \mathrm{T}\ y) = g[f(x\ \mathrm{T}\ y)], & \text{(définition de } g \circ f) \\ = g[f(x)\ \mathrm{T}'\ f(y)], & (f \text{ est un homomorphisme de (E, T) dans (E′, T′))} \\ = g[f(x)]\ \mathrm{T}''\ g[f(y)], & (g \quad — \quad — \quad \text{de (E′, T′) dans (E″, T″))} \\ = (g \circ f)(x)\ \mathrm{T}''\ (g \circ f)(y). & \text{(définition de } g \circ f). \end{array}$$

Si on pose

$$\begin{array}{ll} x' = f(x), & x'' = g(x') = (g \circ f)(x), \\ y' = f(y), & y'' = g(y') = (g \circ f)(y), \end{array}$$

la démonstration précédente se concrétise dans le schéma suivant

$$\begin{array}{ccccc} \mathrm{E} & \xrightarrow{f} & \mathrm{E}' & \xrightarrow{g} & \mathrm{E}'' \\ x & \longmapsto & x' & \longmapsto & x'' \\ y & \longmapsto & y' & \longmapsto & y'' \\ x\ \mathrm{T}\ y & \longmapsto & x'\ \mathrm{T}'\ y' & \longmapsto & x''\ \mathrm{T}''\ y'' \end{array}$$

Démontrons maintenant les résultats suivants :

Théorème 2.

Soit f un homomorphisme de (E, T) dans (E', T')

1. La partie $f(E)$ de E' est stable pour la loi T'.

2. Si la loi T est associative (resp. commutative) alors la loi T' est associative (resp. commutative) **dans $f(E)$.**

3. Si (E, T) possède un élément neutre e alors $f(e)$ est élément neutre pour $(f(E), T')$. Si de plus x et x_1 sont symétriques pour la loi T dans E alors $f(x)$ et $f(x_1)$ sont symétriques pour la loi T' dans $f(E)$.

1. *Quels que soient x' et y' de f(E)* il existe x et y de E tels que $x' = f(x)$, $y' = f(y)$. L'application f étant un homomorphisme de (E, T) dans (E', T') on a donc

$$x' \mathrm{T}' y' = f(x) \mathrm{T}' f(y) = f(x \mathrm{T} y)$$

or $x \mathrm{T} y \in \mathrm{E}$ donc $x' \mathrm{T}' y' \in f(\mathrm{E})$.

2. *Quels que soient x', y', z' de f*(E) il existe x, y, z de E tels que $x' = f(x)$, $y' = f(y)$, $z' = f(z)$. On a donc

$$\begin{aligned}
(x' \mathrm{T}' y') \mathrm{T}' z' &= [f(x) \mathrm{T}' f(y)] \mathrm{T}' f(z) \\
= f(x \mathrm{T} y) \mathrm{T}' f(z) &= f[(x \mathrm{T} y) \mathrm{T} z] && (f \text{ est un homomorphisme}) \\
&= f[x \mathrm{T} (y \mathrm{T} z)] && (\text{la loi T est associative}) \\
= f(x) \mathrm{T}' f(y \mathrm{T} z) &= f(x) \mathrm{T}' [f(y) \mathrm{T}' f(z)] && (f \text{ est un homomorphisme}) \\
&= x' \mathrm{T}' (y' \mathrm{T}' z').
\end{aligned}$$

De même si la loi T est commutative nous avons

$$x' \mathrm{T}' y' = f(x) \mathrm{T}' f(y) = f(x \mathrm{T} y) = f(y \mathrm{T} x) = f(y) \mathrm{T}' f(x) = y' \mathrm{T}' x'.$$

3. Quel que soit x' de f(E) il existe x de E tel que $x' = f(x)$, d'où

$$x' \mathrm{T}' f(e) = f(x) \mathrm{T}' f(e) = f(x \mathrm{T} e) = f(x) = x',$$

et

$$f(e) \mathrm{T}' x' = f(e) \mathrm{T}' f(x) = f(e \mathrm{T} x) = f(x) = x'.$$

Si x et x_1 sont symétriques dans E on a

$$x \mathrm{T} x_1 = x_1 \mathrm{T} x = e$$

l'homomorphisme f nous permet d'écrire

$$\begin{aligned}
f(x \mathrm{T} x_1) &= f(x_1 \mathrm{T} x) = f(e), \\
f(x) \mathrm{T}' f(x_1) &= f(x_1) \mathrm{T}' f(x) = f(e).
\end{aligned}$$

On en déduit immédiatement :

Corollaire 1.

Soit f un homomorphisme de (E, T) dans (E', T') ; si (E, T) est un groupe (resp. un groupe commutatif) alors $(f(E), T')$ est un groupe (resp. un groupe commutatif).

Dans le cas de l'homomorphisme surjectif f de $(\mathbb{Z}, +)$ sur $(\mathbb{Z}/n\mathbb{Z}, +)$ définie pour tout x de $\mathbb{Z}$ par $f(x) = \dot{x}$ on a $\mathbb{Z}/n\mathbb{Z} = f(\mathbb{Z})$; nous retrouvons ainsi que $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif : la démonstration directe donnée au § 2.9 *d* est la même que celle donnée dans les parties du théorème 2; on a simplement remplacé partout $f(x)$ par $\dot{x}$, $f(y)$ par $\dot{y}$, etc.

Vous démontrerez facilement le corollaire suivant :

Corollaire 2.

Soit f un homomorphisme de $(E, +, \times)$ dans $(E', +, \times)$, c'est-à-dire un homomorphisme à la fois pour l'addition et la multiplication.
Si $(E, +, \times)$ est un anneau alors $(f(E), +, \times)$ est un anneau.
Si de plus E est commutatif (resp. unitaire) alors $f(E)$ est commutatif (resp. unitaire).

(En plus des propriétés énoncées dans le théorème 2 il vous faudra démontrer que si la multiplication est distributive par rapport à l'addition dans E alors elle l'est aussi dans $f(E)$. Il faudra partir de trois éléments quelconques x', y', z' de $f(E)$).
Dans le cas de l'homomorphisme surjectif f de $(\mathbb{Z}, +, \times)$ sur $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ étudié plus haut on a $f(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$; nous retrouvons ainsi que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau commutatif unitaire.

REMARQUES

1. L'application f de E dans E', homomorphisme pour les lois définies sur E et E', nous permet de déduire de certaines propriétés de (E, T) des propriétés de T' **uniquement sur $f(E)$.**
2. Les propriétés qui se transmettent de (E, T) à $(f(E), T')$ par l'homomorphisme f, sont celles explicitement mentionnées dans le théorème 2 : il ne faut pas généraliser abusivement.
   Par exemple (cf. § 2.9 f) $(\mathbb{Z}, +, \times)$ est un anneau intègre et l'anneau $\mathbb{Z}/6\,\mathbb{Z}$ possède des diviseurs de zéro. Dans $(\mathbb{Z}, +, \times)$ les seuls éléments inversibles sont 1 et -1 et dans $\mathbb{Z}/5\,\mathbb{Z}$ tous les éléments $\dot{x} \neq \dot{0}$ sont inversibles.
3. L'homomorphisme f de (E, T) dans (E', T') ne nous permet pas, en général, de déduire de certaines propriétés de $(f(E), T')$ des propriétés de (E, T). En effet x', y',z' étant trois éléments de $f(E)$ vérifiant $z' = x'\,T'\,y'$, si ces éléments sont les images respectives par f de x, y, z de E, on peut très bien avoir $z \neq x\,T\,y$.
   Par exemple pour

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}/6\,\mathbb{Z}$$

   on a $\dot{2} \times \dot{3} = \dot{0}$ et

$$\begin{aligned} 8 &\longmapsto \dot{2} \\ -3 &\longmapsto \dot{3} \\ 0 &\longmapsto \dot{0} \end{aligned}$$

   or $8 \times (-3) \neq 0$.

La difficulté signalée à la remarque 1 ci-dessus provient du fait que l'homomorphisme f peut être non surjectif. Celles signalées aux remarques 2 et 3 proviennent du fait que f peut être non injectif.
Toutes ces difficultés disparaissent dans le cas particulier étudié ci-dessous.

d) Isomorphismes.

Définition.

On appelle **isomorphisme** de (E, T) sur (E', T') tout homomorphisme f de (E, T) dans (E', T') possédant les propriétés suivantes :

i. f est une bijection.
ii. f^{-1} est un homomorphisme de (E', T') dans (E, T).

Considérons un *homomorphisme bijectif* de (E, T) sur (E', T').
Quels que soient x' et y' de E', il existe un *élément unique* x de E et un *élément unique* y de E tels que $x' = f(x)$ et $y' = f(y)$. Donc, f étant un homomorphisme, on a

$$f(x\,T\,y) = f(x)\,T'\,f(y) = x'\,T'\,y'.$$

Désignant par f^{-1} la bijection réciproque de f nous aurons

$$x = f^{-1}(x') \quad , \quad y = f^{-1}(y')$$

d'où

$$x \mathrm{T} y = f^{-1}(x' \mathrm{T}' y')$$

c'est-à-dire

$$f^{-1}(x') \mathrm{T} f^{-1}(y') = f^{-1}(x' \mathrm{T}' y')$$

et ceci quels que soient x', y' de E'; donc f^{-1} *est un homomorphisme de* (E', T') *sur* (E, T). Concluons :

Théorème 3.

Pour qu'un homomorphisme f de (E, T) dans (E', T') soit un isomorphisme de (E, T) sur (E', T') il suffit que f soit une bijection.

Si f est un isomorphisme de (E, T), sur (E', T'), alors f^{-1} est un isomorphisme de (E', T') sur (E, T); on dit souvent que, dans ce cas, (E, T) et (E', T') sont *isomorphes;* cette locution commode risque de créer une confusion entre l'isomorphisme f de E sur E' et l'isomorphisme f^{-1} de E' sur E.
Quels que soient x de E et x' de E' on a

$$x' = f(x) \iff x = f^{-1}(x')$$

on voit alors que la loi T sur E et la loi T' sur E' ont exactement les mêmes propriétés.

EXEMPLE 4

Vous connaissez les puissances entières relatives de 2; soit D l'ensemble des nombres rationnels de la forme 2^n où n est un entier relatif quelconque; vous savez que quels que soient n et p de $\mathbb{Z}$ on a $2^{n+p} = 2^n \times 2^p$, et que

$$f : \mathbb{Z} \longrightarrow \mathrm{D}$$
$$n_1 \longrightarrow 2^n$$

est une bijection. Il en résulte que f est un isomorphisme de $(\mathbb{Z}, +)$ sur (D, $\times$). Comme $(\mathbb{Z}, +)$ est un groupe commutatif, il en est de même de (D, $\times$).

La composée de deux bijections est une bijection; le théorème 1 (§ 2.10 c) permet d'énoncer

Le composé de deux isomorphismes est un isomorphisme.

2. 11 NOTION DE CORPS COMMUTATIF

a) Introduction.

Reprenons l'anneau $(\mathbb{Z}/5\,\mathbb{Z}, +, \times)$ étudié au § 2.9 f. Rappelons que l'on a dans $\mathbb{Z}/5\,\mathbb{Z}$

$\dot{x}$	$\dot{1}$	$\dot{2}$	$\dot{3}$	$\dot{4}$
$(\dot{x})^{-1}$	$\dot{1}$	$\dot{3}$	$\dot{2}$	$\dot{4}$

Donc dans $\mathbb{Z}/5\,\mathbb{Z}$ tout élément distinct de $\dot{0}$, élément neutre de l'addition, est inversible.

En construisant la table de multiplication de $\mathbb{Z}/5\,\mathbb{Z}$ (ce que vous avez fait à l'exercice 1 du § 2.9 *c*) vous constatez que

$$(\mathbb{Z}/5\,\mathbb{Z})^* = (\mathbb{Z}/5\,\mathbb{Z}) - \{\dot{0}\} = \{\dot{1},\ \dot{2},\ \dot{3},\ \dot{4}\}$$

est une partie stable de $\mathbb{Z}/5\,\mathbb{Z}$ pour la multiplication.
La multiplication est une loi interne associative et commutative dans $(\mathbb{Z}/5\,\mathbb{Z})^*$; elle possède un élément neutre $\dot{1}$ et tout élément est inversible. Donc :
$((\mathbb{Z}/5\,\mathbb{Z})^*, \times)$ *est un groupe commutatif.*

L'ensemble $\mathbb{Z}/5\,\mathbb{Z}$ muni de l'addition et de la multiplication des entiers modulo 5 possède les deux propriétés suivantes
i. $(\mathbb{Z}/5\,\mathbb{Z}, +, \times)$ est un anneau commutatif.
ii. $(\mathbb{Z}/5\,\mathbb{Z})^*, \times)$ est un groupe.
Nous résumerons ces propriétés en disant :
$(\mathbb{Z}/5\,\mathbb{Z}, +, \times)$ *est un corps commutatif.*

b) Définition d'un corps commutatif.

Définition.

On dit qu'un ensemble K, muni de deux lois internes appelées addition et multiplication, est un corps commutatif si et seulement si
i. $(K, +, \times)$ est un anneau commutatif,
ii. $(K^*, \times)$ est un groupe, K^* désignant $K - \{0_K\}$.

Nous dirons souvent « corps », étant entendu qu'il s'agit d'un « corps commutatif ».
Un corps commutatif possède déjà toutes les propriétés d'un anneau; en particulier $(K, +)$ est un groupe commutatif, appelé *groupe additif* du corps. Son élément neutre 0_K est appelé l'*élément zéro* du corps; désignons cet élément simplement par ω.
Le groupe $(K^*, \times)$ est appelé *groupe multiplicatif du corps*, soit e son élément neutre; comme $\omega \notin K^*$ on a $\omega \neq e$; donc **un corps possède au moins deux éléments : ω et e.**
L'élément e est l'élément neutre de la multiplication dans K^*; comme e est un élément de l'anneau K d'élément zéro ω on a comme dans tout anneau (cf. § 2.3 *e*, exercice 2)

$$e\,\omega = \omega\,e = \omega;$$

donc e est élément neutre de la multiplication dans K et non pas seulement dans K^*. On l'appelle *élément-unité* du corps.

Réciproquement soit $(K, +, \times)$ un *anneau commutatif unitaire* d'élément zéro ω et d'élément unité $e \neq \omega$ tel que *tout élément* $x \neq \omega$ *soit inversible.* Montrons que

$$K^* = K - \{\omega\}$$

est une partie stable de K pour la multiplication.
Soit x et y deux éléments de K tels que $xy = \omega$; si $x = \omega$ on a $\omega y = \omega$ comme dans tout anneau; si $x \neq \omega$ d'après l'hypothèse il existe x^{-1} dans K on a donc

$$x^{-1}(xy) = x^{-1}\,\omega = \omega;$$

comme $x^{-1}(xy) = (x^{-1}x)\,y = ey = y$ on a $y = \omega$. Donc dans l'anneau K où tout élément $x \neq \omega$ est inversible on a, pour tout x et tout y de K,

$$(xy = \omega) \Longrightarrow (x = \omega \quad \text{ou} \quad y = \omega);$$

il en résulte que l'on a aussi (implication *contraposée* de la précédente)

$$(x \neq \omega \quad \text{et} \quad y \neq \omega) \Longrightarrow (xy \neq \omega).$$

Donc $K^* = K - \{\omega\}$ est une partie stable de $(K, \times)$; la multiplication étant associative et commutative dans K l'est aussi dans K^*; e, supposé distinct de ω, appartient à K^* enfin tout élément $x \in K^*$ a une inverse $x^{-1} \in K^*$ (car si $x^{-1} = \omega$ on aurait $xx^{-1} = \omega$ et non $xx^{-1} = e$) donc $(K^*, \times)$ est un groupe et $(K, +, \times)$ un corps.

Théorème.

Pour qu'un anneau commutatif unitaire K d'éléments neutres ω et e soit un corps commutatif il faut et il suffit que $\omega \neq e$ et que tout élément distinct de ω soit inversible.

Au cours de la démonstration précédente nous avons rencontré la propriété suivante.

Un corps est dépourvu de diviseurs de zéro.

EXERCICES

1. Expliciter les propriétés fondamentales d'un corps commutatif (on en trouvera 9 : 4 pour l'addition, 4 pour la multiplication, plus la distributivité).
2. Démontrer que $(\mathbb{Z}/2\mathbb{Z}, +, \times)$ est un corps commutatif.
3. Soit $E = \{a, b\}$ un ensemble à deux éléments. Définir une addition et une multiplication dans E de manière que $(E, +, \times)$ soit un corps. En déduire que tous les corps à deux éléments sont isomorphes entre eux.

Nous verrons au § 2.18 b que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps commutatif si et seulement si n est un nombre premier (cf. aussi exercice n° 2.8, fin du chapitre).

REMARQUE

1. Vous démontrerez facilement que si f est un isomorphisme de $(E, +, \times)$ sur $(E', +, \times)$ et si $(E, +, \times)$ est un corps commutatif, alors $(E', +, \times)$ est aussi un corps commutatif (on utilisera les propriétés données au § 2-10).

III Divisibilité dans l'anneau $\mathbb{Z}$ P.G.C.D. et P.P.C.M.

2. 12 DIVISIBILITÉ ET INCLUSION DES IDÉAUX

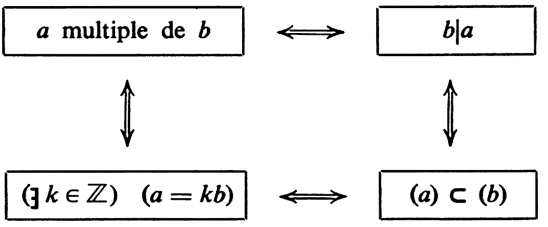
Rappelons que tout idéal de $\mathbb{Z}$ est de la forme $a\mathbb{Z}$ (cf. § 2.7 b). On a $a\mathbb{Z} = (-a)\,\mathbb{Z}$ on peut donc toujours supposer que a est un *entier naturel*. Si $a\mathbb{Z}$ est distinct de l'idéal $\{0\}$ alors $a \in \mathbb{N}^*$; dans ce cas a est le *plus petit entier strictement positif* de l'idéal. L'idéal $a\mathbb{Z}$ comprend, 0, a, $a + a = 2a$, $a + a + a = 3a$ ... $-a$, $-a - a = (-2)\,a$, $-a - a - a = (-3)\,a$ ..., nous dirons qu'il est *engendré* par a. **Nous le noterons aussi (a).**

Étant donnés deux entiers relatifs non nuls a et b, les propriétés suivantes sont équivalentes :

1. a est un multiple de b,
2. b divise a, que l'on écrit $b|a$,
3. $(\exists k \in \mathbb{Z}) \quad (a = kb)$.

Comparons $a\mathbb{Z}$ et $b\mathbb{Z}$, les deux idéaux engendrés respectivement par a et b, *que nous noterons aussi* (a) et (b).

Puisque a est un multiple de b, $a \in b\mathbb{Z}$; et puisque $b\mathbb{Z}$ est un idéal, pour tout nombre $n \in \mathbb{Z}$, $na \in b\mathbb{Z}$. Par suite : $a\mathbb{Z} \subset b\mathbb{Z}$, soit $(a) \subset (b)$.
Inversement, si $(a) \subset (b)$, alors $a \in (b)$ et a est un multiple de b, d'après la définition de (b).
Résumons à l'aide d'un schéma valable quels que soient les entiers relatifs a et b, non nuls :



REMARQUES

1. On a à la fois
$$(6) \subset (2) \quad \text{et} \quad 2 < 6,$$
et d'une manière générale, si a et b sont non nuls :
$$(a) \subset (b) \quad \text{et} \quad |b| \leqslant |a|.$$
2. Quel que soit a de $\mathbb{Z}$ on a $(0) \subset (a)$, ce qui signifie que tout entier divise zéro. C'est pour cette raison que l'on étudie la divisibilité uniquement dans $\mathbb{Z}^*$ (ou $\mathbb{N}^*$).

EXERCICES

1. Démontrer sans utiliser les idéaux que la relation « a divise b » est une relation d'ordre partiel dans $\mathbb{N}^*$ (on démontrera d'abord que le seul élément inversible de $(\mathbb{N}^*, \times)$ est 1).
2. Démontrer la propriété de l'exercice 1 ci-dessus en remarquant qu'à tout idéal de $\mathbb{Z}$ est associé un entier naturel unique.

2. 13 DIVISEURS COMMUNS A DEUX ENTIERS RELATIFS P.G.C.D.

a) Somme de deux idéaux : P.G.C.D. de a et b.

Étant donnés deux entiers relatifs non nuls, a et b, considérons le sous-ensemble I de $\mathbb{Z}$ défini par :
$$\mathrm{I} = \{x \in \mathbb{Z} \mid (\exists\, (u, v) \in \mathbb{Z} \times \mathbb{Z}) \quad (x = au + bv)\}.$$

Cet ensemble se note $\mathrm{I} = a\mathbb{Z} + b\mathbb{Z} = (a) + (b)$; il s'appelle la *somme des idéaux* (a) et (b).
L'ensemble I comprend donc tous les entiers relatifs de la forme $au + bv$ où u et v sont deux entiers relatifs quelconques. Cet ensemble est non vide, puisque, par exemple, $a \in \mathrm{I}$.
Soit x et x' deux éléments quelconques de I. Posons :
$$x = au + bv \quad , \quad x' = au' + bv'.$$

Alors, $x - x' = a(u - u') + b(v - v')$.
On en déduit que
$$(\forall\, (x, x') \in \mathrm{I} \times \mathrm{I}) \quad (x - x' \in \mathrm{I}). \tag{1}$$

D'autre part, étant donné un nombre quelconque z de $\mathbb{Z}$:
$$z \times x = a(uz) + b(vz).$$
D'où :
$$(\forall\, x \in \mathrm{I}) \quad (\forall\, z \in \mathbb{Z}) \quad (xz \in \mathrm{I}). \tag{2}$$

La partie I non vide de $\mathbb{Z}$ vérifiant (1) et (2) est un idéal de $\mathbb{Z}$.
Cet idéal ne peut être égal à l'idéal $\{0\}$ puisqu'il contient $a \neq 0$. L'idéal I est donc l'ensemble des entiers multiples de *son plus petit élément strictement positif* δ donc

$$(a) + (b) = (\delta).$$

Tout élément de (a) peut s'écrire $au + (b \times 0)$. Par suite, $(a) \subset (\delta)$. De même $(b) \subset (\delta)$.
Il en résulte que δ divise a et b; donc δ est un *diviseur commun* à a et b.
D'autre part, $\delta \in a\mathbb{Z} + b\mathbb{Z}$; il existe donc u_0 et v_0 appartenant à $\mathbb{Z}$ tels que :

$$\delta = au_0 + bv_0.$$

On en déduit que, si d est un diviseur commun quelconque de a et b, d divise δ; par suite :
— pour tout diviseur commun d de a et b, $|d| \leqslant \delta$, donc δ est le plus grand diviseur strictement positif commun à a et b.
— tout diviseur commun à a et b est un diviseur de δ.

Définition.

Étant donnés deux entiers relatifs non nuls a et b, le plus petit entier strictement positif qui engendre l'idéal $(a) + (b)$ est appelé **le plus grand diviseur commun à a et b.**

On le notera $\Delta(a, b)$; en abrégé on dira que $\Delta(a, b)$ est *le* p.g.c.d. de a et b.
Concluons l'étude précédente.

Théorème.

1. L'ensemble des diviseurs communs à a et b est égal à l'ensemble des diviseurs de $\Delta(a, b)$.
2. Il existe des entiers relatifs u_0 et v_0 tels que :

$$\Delta(a, b) = au_0 + bv_0.$$

REMARQUE

1. Nous montrerons plus loin que le couple (u_0, v_0) n'est pas unique.

b) Entiers premiers entre eux.

Soit deux entiers non nuls a et b tels que $\Delta(a, b) = 1$; les seuls diviseurs communs sont 1 et -1; réciproquement si les seuls diviseurs communs sont 1 et -1 alors $\Delta(a, b) = 1$.
D'autre part d'après l'étude précédente la relation $\Delta(a, b) = 1$ est équivalente à

$$(a) + (b) = (1) = \mathbb{Z},$$

c'est-à-dire à la relation : il existe u_0 et v_0 de $\mathbb{Z}$ tels que $au_0 + bv_0 = 1$; concluons

Théorème et définition.

Quels que soient les entiers non nuls a et b les propriétés suivantes sont équivalentes :
1. a et b ont pour seuls diviseurs communs 1 et -1.
2. $\Delta(a, b) = 1$.
3. $(a) + (b) = \mathbb{Z}$.
4. Il existe u_0 et v_0 de $\mathbb{Z}$ tels que

$$au_0 + bv_0 = 1.$$

Deux entiers non nuls vérifiant l'une de ces propriétés sont appelés entiers **premiers entre eux** ou encore **entiers étrangers.**

L'égalité $au_0 + bv_0 = 1$ est appelée **égalité de Bezout**. Elle montre que u_0 et v_0 sont étrangers. Nous montrerons plus loin que le couple (u_0, v_0) n'est pas unique.

c) Conséquences de la définition du p.g.c.d.

1. Soient trois entiers relatifs *non nuls* a, b, c. Posons

$$(a) + (b) = (\delta) \quad \text{avec} \quad \delta = \Delta(a, b) > 0,$$
$$(ca) + (cb) = (\delta') \quad \text{avec} \quad \delta' = \Delta(ca, cb) > 0.$$

L'idéal (δ') est l'ensemble des entiers relatifs de la forme $(ca)\,u + (cb)\,v = c\,(au + bv)$ où u et v sont deux entiers relatifs quelconques. Or l'ensemble des entiers $au + bv$ est l'ensemble des multiples entiers de δ. Donc l'idéal (δ') est l'ensemble des multiples entiers de $c\delta$; comme $\delta > 0$ et $\delta' > 0$ on a donc $\delta' = |c|\,\delta$. D'où

$$\Delta(ca,\ cb) = |c|\,\Delta(a,\ b).$$

Soit d un diviseur commun à a et b posons

$$a = a'd \quad \text{c'est-à-dire} \quad a' = \frac{a}{d} \in \mathbb{Z}$$
$$b = b'd \quad \text{—} \quad b' = \frac{b}{d} \in \mathbb{Z}$$

la formule précédente nous donne

$$\Delta(a'd,\ b'd) = |d|\,\Delta(a',\ b')$$

Théorème.

Étant donnés deux entiers relatifs non nuls quelconques a et b, pour tout entier relatif non nul c et pour tout diviseur d commun à a et b on a

$$\Delta(ca, cb) = |c|\,\Delta(a, b),$$
$$\Delta\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{\Delta(a, b)}{|d|}.$$

La condition $\Delta\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ est équivalente à $\Delta(a, b) = |d|$; concluons

Corollaire.

Soit d un diviseur commun à a et b entiers relatifs non nuls; $|d|$ est le p.g.c.d. de a et b si et seulement si les entiers $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux.

EXERCICE 1

Trouver les couples d'*entiers naturels* (a, b) sachant que $a + b = 56$ et $\Delta(a, b) = 7$.

2. Soit a, b et c trois entiers relatifs non nuls tels que $\Delta(a, b) = 1$ et $\Delta(a, c) = 1$. Calculons $\Delta(a, bc)$. Nous avons quels que soient a et b

$$\Delta(a, b) = 1 \iff [\exists\,(u_0, v_0) \in \mathbb{Z} \times \mathbb{Z}) \quad (au_0 + bv_0 = 1)].$$

Multiplions par c les deux membres de la dernière égalité. On obtient :

$$a\,(cu_0) + (bc)\,v_0 = c.$$

Tout diviseur commun à a et bc divise c, donc a et c et par suite, il divise $\Delta(a, c) = 1$. Il est donc égal à 1 ou -1, donc $\Delta(a, bc) = 1$.

Théorème.

Quels que soient les entiers relatifs non nuls a, b, c on a

$$\left.\begin{array}{l}\Delta(a,\ b) = 1\\ \text{et}\quad \Delta(a,\ c) = 1\end{array}\right\} \Longrightarrow \Delta(a,\ bc) = 1.$$

EXERCICE 2

Démontrer que, quels que soient les entiers relatifs non nuls a, b, c on a

$$\left.\begin{array}{l}\Delta(a,\ b) = \delta\\ \text{et}\quad \Delta(a,\ c) = 1\end{array}\right\} \Longrightarrow \Delta(a,bc) = \delta.$$

En faisant $b = c$ on obtient

Corollaire.

Quels que soient les entiers relatifs non nuls a et b on a

$$[\Delta(a,\ b) = 1] \Longrightarrow [\Delta(a,\ b^2) = 1].$$

EXERCICE 3

En raisonnant par récurrence, on établira que :

α) Quels que soient les entiers relatifs non nuls a et b et quel que soit l'entier naturel non nul n on a

$$[\Delta(a,\ b) = 1] \Longrightarrow [\Delta(a,\ b^n) = 1].$$

β) Quels que soient les entiers relatifs non nuls a et b et quels que soient les entiers naturels non nuls n et p on a

$$[\Delta(a,\ b) = 1] \Longrightarrow [\Delta(a^n,\ b^p) = 1].$$

3. Théorème de GAUSS.

Supposons qu'un nombre entier relatif d divise un produit ab, et que $\Delta(d,\ a) = 1$. Puisque $\Delta(d,\ a) = 1$, il existe des nombres entiers relatifs u_0 et v_0 tels que

$$du_0 + av_0 = 1,$$

d'où, par multiplication par b :

$$b\,d\,u_0 + ab\,v_0 = b.$$

Le nombre d divise d et ab donc, d'après cette égalité, il divise b.

Théorème de Gauss.

Quels que soient les entiers relatifs non nuls a, b, d on a

$$\left.\begin{array}{l}d \mid ab\\ \text{et}\quad \Delta(a,\ d) = 1\end{array}\right\} \Longrightarrow (d \mid b).$$

Application. Trouver tous les couples $(u,\ v) \in \mathbb{Z} \times \mathbb{Z}$ *tels que*

(1) $$5\,u + 3\,v = 1.$$

Nous savons qu'il en existe puisque $\Delta(5,\ 3) = 1$. En particulier l'un de ces couples est $(2,\ -\ 3)$ car

(1′) $$5 \times 2 + 3 \times (-\ 3) = 1.$$

En retranchant (1′) de (1) on obtient

$$5(u - 2) + 3(v + 3) = 0$$

soit

$$5(u - 2) = -\ 3(v + 3).$$

L'entier 5 divise $-3(v+3)$ et est premier avec -3, il divise donc $v+3$; par conséquent il existe un entier k tel que $v+3=5k$; on en déduit $u-2=-3k$; on a donc

$$u=2-3k \quad \text{et} \quad v=-3+5k;$$

réciproquement quel que soit $k \in \mathbb{Z}$ on a bien $5u+3v=1$.
L'ensemble des solutions de (1) est donc l'ensemble des couples $(2-3k, -3+5k)$ où k est un entier relatif arbitraire.

REMARQUE 2

Cet exemple montre que, a et b étant premiers entre eux, il y a une infinité de couples (u, v) tels que $au+bv=1$. Si (u_0, v_0) est l'un d'entre eux tous les autres sont de la forme (u_0-bk, v_0+ak) où k est un entier relatif quelconque.
Le difficile est de trouver une solution, on peut procéder par tâtonnement; nous indiquerons une méthode générale au 2.14 b.
On peut aussi remarquer que la relation (1) (dans $\mathbb{Z}$) est équivalente à la relation (2)

(2) $$5u \equiv 1 \pmod 3$$

ou encore à la relation (3) (dans $\mathbb{Z}/3\mathbb{Z}$)

(3) $$\dot{5}\dot{u}=\dot{1} \quad \text{ou} \quad \dot{2}\dot{u}=\dot{1}$$

et on trouve $\dot{u}=\dot{2}$, d'où $u \equiv 2 \pmod 3$. Cette méthode n'est pratique que si l'un des nombres a ou b est « petit ».

EXERCICE 4

Trouver tous les couples $(x, y) \in \mathbb{N} \times \mathbb{N}$ tels que

$$4x-7y=1.$$

2. 14 DÉTERMINATION PRATIQUE DE $\Delta(a, b)$

Les diviseurs de l'entier relatif x étant les mêmes que ceux de $-x$ nous supposerons a et b **strictement positifs.**

a) Algorithme d'Euclide.

Premier cas : *b divise a.* Il existe un entier unique tel que

$$a=bq.$$

L'ensemble des diviseurs communs à a et b est identique à l'ensemble des diviseurs de b donc

$$\Delta(a, b)=b.$$

Deuxième cas : *b ne divise pas a.* Alors il existe q et r tels que

$$a=bq+r \quad \text{et} \quad 0<r<b.$$

Tout diviseur commun à a et b divise $r=a-bq$; réciproquement tout diviseur commun à b et r divise $a=bq+r$; donc l'ensemble des diviseurs communs à a et b est identique à l'ensemble des diviseurs communs à b et r; en particulier $\Delta(a, b)=\Delta(b, r)$.

Lemme.

Soit a et b deux entiers naturels non nuls, b ne divisant pas a; si r est le reste dans la division euclidienne de a par b on a

$$\Delta(a, b)=\Delta(b, r).$$

EXEMPLES

1) Cherchons $\Delta(795, 53)$.
Divisons 795 par 53. Nous trouvons :

$$795 = 15 \times 53.$$

D'après le résultat trouvé dans le premier cas ci-dessus, il résulte que $\Delta(795, 53) = 53$.

2) Cherchons $\Delta(1\,971, 63)$.
Procédons de la même façon que précédemment ; divisons 1 971 par 63. Nous obtenons :

$$1\,971 = (31 \times 63) + 18. \quad \text{D'où} : \Delta(1\,971, 63) = \Delta(63, 18).$$

De même :

$$63 = (3 \times 18) + 9. \quad \text{D'où} \quad \Delta(63, 18) = \Delta(18, 9).$$
$$18 = 2 \times 9. \quad \text{Donc} \quad \Delta(18, 9) = 9.$$

Concluons : $\Delta(1\,971, 63) = 9$.

Généralisons ce procédé.

Algorithme d'EUCLIDE ou méthode des « divisions successives ».
Soit a et b deux entiers naturels non nuls. On se propose de calculer $\Delta(a, b)$.
Effectuons la division euclidienne de a par b.
Deux cas sont possibles, qui s'excluent :

$$a = bq \quad , \quad r = 0; \quad \text{alors} \quad \Delta(a, b) = b.$$
$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b; \quad \text{alors} \quad \Delta(a, b) = \Delta(b, r_1).$$

Dans le premier cas, le problème est résolu.
Dans le second cas, on recommence l'opération comme dans le second exemple : on divise b par r_1. On obtient ainsi, successivement, si les restes obtenus sont *non nuls* :

$$a = bq_1 + r_1 \quad , \quad 0 < r_1 < b \quad , \quad \Delta(a, b) = \Delta(b, r_1)$$
$$b = r_1 q_2 + r_2 \quad , \quad 0 < r_2 < b \quad , \quad \Delta(b, r_1) = \Delta(r_1, r_2)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$r_{n-2} = r_{n-1} q_n + r_n \quad , \quad 0 < r_n < r_{n-1} \quad , \quad \Delta(r_{n-2} r_{n-1}) = \Delta(r_{n-1}, r_n)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Des inégalités concernant les restes, il résulte que l'on a

$$0 < r_n < r_{n-1} < \ldots < r_1 < b.$$

Les restes obtenus constituent une suite de nombres entiers positifs *strictement décroissante*. Au bout d'un certain nombre de divisions, on trouvera donc un reste nul. Supposons $r_n \neq 0$ et $r_{n+1} = 0$. On a

$$r_{n-1} = r_n q_{n+1} \quad \text{d'où} \quad \Delta(r_{n-1}, r_n) = r_n.$$

Des égalités concernant les plus grands diviseurs communs aux couples de nombres, il résulte que :

$$\Delta(a, b) = r_n.$$

Le plus grand diviseur commun à a et b est le dernier reste non nul dans la méthode des divisions successives de a par b.

Si on trouve $r_n = 1$, a et b sont premiers entre eux.

Exemple et disposition pratique : recherche de $\Delta(2375, 75)$.

	31	1	2	← quotients
2 375	75	50	25	← diviseurs
125	25	0		← restes
50				

EXERCICES

Rechercher $\Delta(a, b)$ pour les valeurs suivantes de a et b :

1. $a = 871$, $b = 533$.
2. $a = 285$, $b = 322$.
3. $a = 1\,812$, $b = 537$.

b) Exercice résolu.

Résolution de l'équation :

$$437\,x - 241\,y = 1,$$

où x et y représentent des entiers relatifs.

Il faut d'abord déterminer une solution particulière de cette équation. Nous utiliserons l'algorithme d'Euclide relatif aux deux nombres 437 et 241 ; nous obtenons successivement (fig. 2).

fig. 2

−75	$437 = (1 \times 241) + 196$	(1)
61	$241 = (1 \times 196) + 45$	(2)
−14	$196 = (4 \times 45) + 16$	(3)
5	$45 = (2 \times 16) + 13$	(4)
− 4	$16 = (1 \times 13) + 3$	(5)
1	$13 = (4 \times 3) + 1$	(6)

Les nombres 437 et 241 étant premiers entre eux, les couples (x, y) existent.
Exprimons 1 à l'aide des deux nombres 437 et 241, en multipliant chaque égalité précédente par un nombre convenablement choisi, de telle sorte que les nombres : 3, 13, 16, 45, 196 se trouvent éliminés lorsqu'on ajoutera membre à membre les 6 égalités. On choisira d'abord le coefficient multiplicatif (— 4) pour l'égalité (5) de telle sorte que 3 soit éliminé, puis (+ 5) pour l'égalité (4) de telle sorte que 13 soit éliminé, et ainsi de suite. D'où :

$$(-75) \times 437 = [(-136) \times 241] + 1,$$

ou encore :

$$(-75) \times 437 - (-136) \times 241 = 1.$$

Le couple (— 75, — 136) est une solution particulière de l'équation donnée. On peut donc écrire :

$$437\,x - 241\,y = [(-75) \times 437] - [(-136) \times 241]$$

ce qui équivaut à :

$$437\,(x + 75) = 241\,(y + 136).$$

On montrera que la solution générale (x, y) est donnée par :

$$\begin{cases} x = 241\,k - 75 \\ y = 437\,k - 136 \end{cases}$$

où k est un entier relatif quelconque.

2. 15 DIVISEURS COMMUNS A k ENTIERS RELATIFS, P.G.C.D.

a) Somme des idéaux (a_1), (a_2), ..., (a_k). p.g.c.d. de a_1, a_2, ..., a_k.

Soit $a_1, a_2, \ldots, a_k$ des nombres relatifs non nuls quelconques.
Considérons le sous-ensemble I de $\mathbb{Z}$ défini par :

$$I = \{x \in \mathbb{Z} \mid (\exists (u_1, u_2, \ldots, u_k) \in \mathbb{Z}^k) \quad (x = a_1u_1 + a_2u_2 + \ldots + a_ku_k)\}.$$

Cet ensemble est noté $I = a_1\mathbb{Z} + a_2\mathbb{Z} + \ldots + a_k\mathbb{Z}$, ou
$I = (a_1) + (a_2) + \ldots + (a_k)$.

On l'appelle **somme** des idéaux (a_1), (a_2), ..., (a_k).

On démontrera, comme on l'a fait dans le cas de la somme de deux idéaux, que I est un idéal de $\mathbb{Z}$. Cet idéal I est distinct de l'idéal $\{0\}$ car I comprend $a_1, \ldots, a_n$ non nuls.
Cet idéal I est donc l'ensemble des multiples de son plus petit élément strictement positif δ.
Donc on a

$$(a_1) + (a_2) + \ldots + (a_k) = (\delta).$$

Tout élément de (a_i) $(1 \leqslant i \leqslant n)$ peut s'écrire :

$$(0 \times a_1) + \ldots + (0 \times a_{i-1}) + u_ia_i + (0 \times a_{i+1}) + \ldots + (0 \times a_k).$$

Donc, *quel que soit i*, $(a_i) \subset (\delta)$ et *par suite* $\delta \mid a_i$.

D'autre part $\delta \in I = (a_1) + \ldots + (a_k)$; il existe donc des entiers $v_1, v_2, \ldots, v_k$ tels que

$$\delta = a_1v_1 + a_2v_2 + \ldots + a_kv_k.$$

Il en résulte que, si d est un diviseur commun quelconque de $a_1, a_2, \ldots, a_k$, d divise δ. par suite :

- pour tout diviseur commun d de $a_1, \ldots, a_k$, $|d| \leqslant \delta$, donc δ est le plus grand diviseur strictement positif commun à $a_1, a_2, \ldots, a_k$.
- tout diviseur commun à $a_1, \ldots, a_k$ est un diviseur de δ.

Définition.

Étant donnés des entiers relatifs non nuls $a_1, a_2, \ldots, a_k$, le plus petit entier strictement positif δ qui engendre l'idéal $(a_1) + (a_2) + \ldots + (a_k)$ est appelé **le plus grand diviseur commun à** $a_1, a_2, \ldots, a_k$.

On le note $\delta = \Delta(a_1, a_2, \ldots, a_k)$; en abrégé on dira que δ est *le* p.g.c.d. de $a_1, a_2, \ldots, a_k$;

Concluons l'étude précédente.

Théorème.

1. L'ensemble des diviseurs communs à $a_1, a_2, \ldots, a_k$ est l'ensemble des diviseurs de $\Delta(a_1, a_2, \ldots, a_k)$.
2. Il existe des entiers relatifs $v_1, v_2, \ldots, v_k$ tels que

$$\delta = a_1v_1 + a_2v_2 + \ldots + a_kv_k.$$

REMARQUE 1

Pour $k > 2$, de même que pour $k = 2$, les entiers $v_1, v_2, \ldots, v_k$ ne sont pas déterminés d'une manière unique.

b) Entiers premiers entre eux dans leur ensemble.

Soit des entiers relatifs $a_1, a_2, \ldots, a_k$ non nuls tels que $\Delta(a_1, a_2, \ldots, a_k) = 1$; les seuls diviseurs communs sont 1 et -1; réciproquement si l'ensemble des diviseurs communs à $a_1, \ldots, a_k$ est $\{1, -1\}$, alors $\Delta(a_1, \ldots, a_k) = 1$.
D'autre part, d'après l'étude précédente, la relation $\Delta(a_1, \ldots, a_k) = 1$ est équivalente à

$$(a_1) + (a_2) + \ldots + (a_k) = (1) = \mathbb{Z}$$

c'est-à-dire à la relation : il existe des entiers relatifs $v_1, v_2, \ldots, v_k$ tels que

$$a_1v_1 + a_2v_2 + \ldots + a_kv_k = 1;$$

concluons

Théorème et définition.

Quels que soient les entiers non nuls $a_1, a_2, \ldots, a_k$ les propriétés suivantes sont équivalentes :

1. $a_1, a_2, \ldots, a_k$ ont pour seuls diviseurs communs 1 et -1.
2. $\Delta(a_1, a_2, \ldots, a_k) = 1$.
3. $(a_1) + (a_2) + \ldots + (a_k) = \mathbb{Z}$.
4. Il existe des entiers relatifs $v_1, v_2, \ldots, v_k$ tels que

$$a_1v_1 + a_2v_2 + \ldots + a_kv_k = 1.$$

Les entiers relatifs non nuls $a_1, a_2, \ldots, a_k$ vérifiant l'une de ces propriétés sont appelés **entiers premiers entre eux dans leur ensemble,** ou encore **entiers étrangers dans leur ensemble.**

REMARQUE 2

Les deux propriétés
P_1 : $a_1, a_2, \ldots, a_k$ sont premiers entre eux dans leur ensemble,
P_2 : $a_1, a_2, \ldots, a_k$ sont premiers entre eux deux à deux,
ne sont pas équivalentes.
Par exemple 14, -10, 35 vérifient P_1 mais ne vérifient pas P_2 car $\Delta(14, -10) = 2$, $\Delta(-10, 35) = 5$, $\Delta(35, 14) = 7$.
En revanche P_2 implique toujours P_1, on dit que la propriété P_2 est plus forte que la propriété P_1.

c) Exercice résolu.

Détermination de $\Delta(315, 225, 525)$.

L'ensemble des diviseurs communs à 315, 225, 525 est l'intersection des ensembles des diviseurs de ces trois nombres. L'intersection étant une opération associative dans $\mathfrak{T}(\mathbb{Z})$, il est donc possible de déterminer d'abord l'intersection des ensembles des divi-

seurs de 315 et de 225, c'est-à-dire l'ensemble des diviseurs de $\Delta(315, 225) = \delta$. Puis, il suffit ensuite de déterminer l'intersection des ensembles de diviseurs de δ et 525, c'est-à-dire l'ensemble des diviseurs de $\Delta(315, 225, 525)$.

Calculons δ :

	1	2	2
315	225	90	45
90	45	0	

D'où $\Delta(315, 225) = 45$.

Calculons $\Delta(45, 525)$.

	11	1	2
525	45	30	15
75	15	0	
30			

D'où : $\Delta(45, 525) = 15$ et, par suite,

$$\Delta(315, 225, 525) = 15.$$

Le procédé se généralise de lui-même pour la recherche de $\Delta(a_1, a_2, \ldots, a_k)$ comme vous le montrerez en résolvant l'exercice suivant.

EXERCICE

Démontrer que dans $\mathbb{Z}^*$, $(a, b) \longmapsto \Delta(a, b)$ est une loi de composition interne associative et commutative.
En déduire que si on pose $\delta_i = \Delta(a_1, a_2, \ldots, a_i)$ pour $2 \leqslant i \leqslant k$, on a, pour tout i, tel que $2 \leqslant i \leqslant k - 1$,

$$\delta_{i+1} = \Delta(\delta_i, a_{i+1}).$$

2.16 MULTIPLES COMMUNS A DEUX OU PLUSIEURS ENTIERS RELATIFS. P.P.C.M.

a) Multiples communs à deux nombres. Intersection de deux idéaux de $\mathbb{Z}$.

Soit a et b deux nombres entiers relatifs non nuls. Les idéaux (a) et (b) engendrés par ces deux nombres sont, respectivement, l'*ensemble des multiples de a* et l'*ensemble des multiples de b*. L'ensemble des multiples communs à a et b est donc $(a) \cap (b)$. Cet ensemble n'est pas vide, puisque, par exemple, $ab \in (a) \cap (b)$.
Soit deux éléments quelconques m et m' de $(a) \cap (b)$. Cela signifie qu'il existe des entiers h, h', k, k' tels que :

$$m = ha = kb \quad \text{et} \quad m' = h'a = k'b.$$

D'où $m - m' = (h - h')\, a = (k - k')\, b$, soit $m - m' \in (a) \cap (b)$.
De même, si z est un entier relatif quelconque on a

$$mz = hza = kzb; \quad \text{donc} \quad mz \in (a) \cap (b).$$

Nous venons d'établir les trois propriétés suivantes :

1. $(a) \cap (b) \neq \varnothing$
2. $(\forall\, m,\ m' \in (a) \cap (b))\quad (m - m' \in (a) \cap (b))$
3. $(\forall\, m \in (a) \cap (b))\quad (\forall\, z \in \mathbb{Z})\quad (mz \in (a) \cap (b))$.

Par suite $(a) \cap (b)$ est un idéal de $\mathbb{Z}$. Cet idéal I est distinct de l'idéal $\{0\}$ car comme nous venons de le voir $ab \in (a) \cap (b)$ et nous avons supposé $a \neq 0$ et $b \neq 0$, donc $ab \neq 0$. Il est donc *engendré par son plus petit élément strictement positif* μ. D'où

$$(a) \cap (b) = (\mu).$$

Définition.

Quels que soient les entiers relatifs non nuls a et b, le plus petit élément strictement positif qui engendre l'idéal $(a) \cap (b)$ est appelé **le plus petit multiple commun à a et b.**

On le notera M (a, b); en abrégé on dira que M (a, b) est *le* p.p.c.m. de a et b. Concluons l'étude précédente.

Théorème.

L'ensemble des multiples communs à deux entiers relatifs non nuls a et b est égal à l'ensemble des multiples de leur plus petit multiple commun.

b) Propriétés de M (a, b).

1. *Comparons* M (a, b) *et* M (ka, kb), où k est un entier relatif non nul quelconque. Posons M $(a, b) = \mu$ et M $(ka, kb) = \mu'$. Rappelons que $\mu > 0$ et $\mu' > 0$; nous avons

$$(a) \cap (b) = (\mu) \qquad \text{et} \qquad (ka) \cap (kb) = (\mu').$$

Soit m' un élément quelconque de (μ'). Il existe deux entiers α et β tels que :

$$\begin{aligned} m' &= \alpha\,(ka) = \beta\,(kb) \\ &= k\,(\alpha a) = k\,(\beta b) \end{aligned}$$

Il existe donc un entier $m = \alpha a = \beta b$ tel que $m' = km$; m est un multiple commun à a et b, il existe donc un entier k' tel que $m = k'\mu$; finalement on a $m' = k\,(k'\mu)$ ou

$$m' = (kk')\,\mu.$$

Tout élément de $(ka) \cap (kb)$ est donc un multiple de $k\,\mu$ et par suite :

$$(ka) \cap (kb) \subset (k\,\mu).$$

Inversement, soit m'' un élément quelconque de $(k\,\mu)$. Il existe un entier k'' tel que :

$$m'' = k''\,(k\,\mu) = k\,(k''\mu).$$

Le nombre $k''\,\mu$ étant un multiple de μ, il existe des entiers α' et β' tels que :

$$\begin{aligned} k''\mu &= \alpha' a = \beta' b, \quad \text{d'où :} \\ m'' &= k\,(\alpha' a) = k\,(\beta' b) \\ &= \alpha'(ka) = \beta'\,(kb). \end{aligned}$$

Tout élément de $(k\mu)$ est donc un élément de $(ka) \cap (kb)$, et par suite

$$(k\mu) \subset (ka) \cap (kb).$$

De ces deux inclusions, il résulte que

$$(k\mu) = (ka) + (kb) = (\mu').$$

Par suite $\mu' = |k|\mu$ (car nous supposons $\mu > 0$ et $\mu' > 0$).

Théorème.

Quels que soient les entiers relatifs non nuls a, b, k on a

$$M(ka, kb) = |k| M(a, b).$$

EXERCICE 1

Si d est un diviseur commun à a et b démontrer que

$$M\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{M(a, b)}{|d|}.$$

(On pourra poser $a = a'd$, $b = b'd$).

2. *Relation entre* $\Delta(a, b) = \delta$ *et* $M(a, b) = \mu$.

Nous avons démontré au § 2.13 c que l'on a, quelque soit l'entier $k \neq 0$,

$$|k| \Delta(a, b) = \Delta(ka, kb).$$

Appliquons cette relation à $k = M(a, b)$; on obtient :

$$M(a, b)\,\Delta(a, b) = \Delta[aM(a, b) \quad , \quad bM(a, b)]$$

soit :

$$\mu\delta \quad = \Delta[M(a^2, ab) \quad , \quad M(ab, b^2)].$$

L'entier ab divise $M(a^2, ab)$ et $M(ab, b^2)$, il divise donc $\Delta[M(a^2, ab), \quad M(ab, b^2)]$, et par conséquent il divise $\mu\delta$.

De même, quel que soit l'entier $k \neq 0$ on a

$$|k| M(a, b) = M(ka, kb).$$

Appliquons cette relation à $k = \Delta(a, b)$; on obtient

$$\Delta(a, b)\, M(a, b) = M[a\Delta(a, b) \quad , \quad b\,\Delta(a, b)]$$

soit :

$$\delta\mu \quad = M[\Delta(a^2, ab) \quad , \quad \Delta(ab, b^2)].$$

L'entier ab est un multiple de $\Delta(a^2, ab)$ et de $\Delta(ab, b^2)$, c'est donc un multiple de

$$M[\Delta(a^2, ab) \quad , \quad \Delta(ab, b^2)],$$

donc un multiple de $\mu\delta$.

On a donc : ab divise $\mu\delta$ et ab est un multiple de $\mu\delta$. Par suite $|ab| = \mu\delta$, car

$$\mu > 0 \quad \text{et} \quad \delta > 0.$$

Théorème.

Quels que soient les entiers relatifs non nuls a et b on a

$$\Delta(a, b) \times M(a, b) = |ab|.$$

On voit que $M(a, b) = |ab|$ si et seulement si $\Delta(a, b) = 1$.

Corollaire.

Le plus petit multiple commun aux entiers non nuls a et b est $|ab|$ si et seulement si ces entiers sont premiers entre eux.

3. *Détermination pratique de* M (a, b).

D'après la relation que nous venons de démontrer, entre $\Delta(a, b)$ et M (a, b), il suffit de connaître $\Delta(a, b)$ pour pouvoir calculer M (a, b).

Exemple : $a = 840$, $b = 320$.
L'algorithme d'Euclide donne les résultats suivants :

	2	1	1	1	2
840	320	200	120	80	40
200	120	80	40	0	

Donc $\Delta(840, 320) = 40$.

Par suite, $M(840, 320) = \dfrac{840 \times 320}{40}$

soit : $M(840, 320) = 6\,720$.

EXERCICE 2

Déterminer M (a, b) dans les cas suivants :
$\alpha)$ $a = 715$, $b = 325$;
$\beta)$ $a = 533$, $b = 697$;
$\gamma)$ $a = 1\,789$, $b = 1\,515$.

4. *Multiples communs à plusieurs entiers. Intersection des idéaux* (a_1), (a_2), ..., (a_k).
Soit $a_1, a_2, \ldots, a_k$ des entiers relatifs non nuls. L'idéal (a_i), où $i \in \{1, 2, \ldots, k\}$, est l'ensemble des multiples de a_i.
L'ensemble $I = (a_1) \cap (a_2) \cap \ldots \cap (a_k)$ est donc l'ensemble des *multiples communs* à $a_1, a_2, \ldots, a_k$. I contient $a_1\, a_2 \ldots a_k \neq 0$, donc I est non vide et est distinct de l'idéal $\{0\}$.
Comme dans le cas où $k = 2$, si $k > 2$, on démontrera que cet ensemble est un idéal de $\mathbb{Z}$ et par suite, qu'il est engendré par son plus petit élément strictement positif μ.
Soit : $(a_1) \cap (a_2) \cap \ldots \cap (a_k) = (\mu)$.

Définition.

Quels que soient les entiers relatifs non nuls $a_1, a_2, \ldots, a_k$, le plus petit élément strictement positif de $(a_1) + \ldots + (a_k)$ est appelé **plus petit multiple commun à** $a_1, a_2, \ldots, a_k$.

On le note M $(a_1, a_2, \ldots, a_k)$. Comme dans le cas $k = 2$, pour $k > 2$ on peut conclure :

Théorème.

L'ensemble des multiples commun à k entiers relatifs non nuls $a_1, a_2, \ldots, a_k$ est égal à l'ensemble des multiples de leur plus petit multiple commun.

Vous calculerez facilement M $(a_1, a_2, \ldots, a_k)$ en utilisant l'exercice suivant.

EXERCICE 3

Démontrer que dans $\mathbb{Z}^*$, $(a, b) \longmapsto M(a, b)$ est une loi de composition interne associative et commutative.
En déduire que si on pose $\mu_i = M(a_1, a_2, \ldots, a_i)$ pour $2 \leqslant i \leqslant k$, on a, pour tout i tel que $2 \leqslant i \leqslant k - 1$,

$$\mu_{i+1} = M(\mu_i, a_{i+1}).$$

IV. Nombres premiers

2.17 NOMBRES PREMIERS

a) Définition et premières propriétés.

Définition.

Un entier relatif n est **premier** si et seulement s'il admet exactement quatre diviseurs $1, -1, n$ et $-n$.

L'entier 0 n'est pas premier puisqu'il admet tout entier pour diviseur.
Les entiers 1 et -1 ne sont pas premiers puisqu'ils n'admettent que deux diviseurs 1 et -1.
L'entier 2 est premier : ses diviseurs sont $1, -1, 2$ et -2.
L'entier 6 n'est pas premier : ses diviseurs sont $1, -1, 2, -2, 3, -3, 6, -6$.
Soit n un entier relatif non premier et distinct de 0, 1 et -1; il admet donc des diviseurs distincts de $+1, -1, n$ et $-n$. Soit d le diviseur le plus petit possible tel que $1 < d < |n|$.
Démontrons que d est premier. Si d n'est pas premier, il existe un entier d' tel que $1 < d' < d$ et qui divise d donc n. Ceci est en contradiction avec le fait que l'on a choisi pour d le plus petit diviseur de n tel que $1 < d < |n|$. Donc d est premier.
Si $n = 0$ il est divisible par tout entier relatif donc 0 a des diviseurs premiers.
Enfin si n est premier il admet n comme diviseur premier. Concluons.

Théorème.

Tout entier relatif distinct de 1 et -1 admet au moins un diviseur premier.

Soit P l'ensemble des *nombres premiers positifs*; cet ensemble n'est pas vide car $2 \in P$. Si cet ensemble était fini, il serait majoré (cf. § 1. 6 c); donc il aurait un plus grand élément n.
Considérons le nombre $n' = n! + 1$.

- Si n' est premier, on a trouvé n' premier tel que $n' > n$.
- Si n' n'est pas premier il admet un diviseur premier p. Cet entier est distinct de $2, 3, \ldots, n$ car chacun de ces entiers divise $n!$, ne divise pas 1, donc ne divise pas $n' = n! + 1$.

Donc dans ce cas aussi nous avons mis en évidence un nombre premier $p > n$.
Notre hypothèse est donc fausse; P est donc infini.

Théorème.

L'ensemble des nombres premiers est infini.

b) Étant donné un entier n cherchons à déterminer de façon pratique si n **est premier ou non.**

Les diviseurs de n étant ceux de $-n$, nous supposerons $n \in \mathbb{N}^*$.
Soit $n > 1$ non premier et d le *plus petit* diviseur de n tel que $1 < d < n$. On a $n = dk$ et par conséquent $d \leqslant k$, donc $d^2 \leqslant dk$ c'est-à-dire $d^2 \leqslant n$. Or nous avons vu ci-dessus que d est premier; concluons.

Lemme.
Tout entier $n > 1$ non premier admet au moins un diviseur premier d vérifiant $d^2 \leqslant n$.

Ce résultat va nous aider à reconnaître si n est premier ou non.

Premier cas : $n < 100$ (crible d'ERATOSTHÈNE).

Formons un tableau contenant les nombres entiers n tels que $0 \leqslant n < 100$; ces nombres étant écrits dans le système décimal; le nombre des dizaines figure dans la colonne de gauche marquée d et le nombre des unités est indiqué dans la ligne supérieure marquée u (fig. 3).

fig. 3

d \ u	0	1	2	3	4	5	6	7	8	9
0			2	3		5		7		
1		11		13				17		19
2				23						29
3		31						37		
4		41		43				47		
5				53						59
6		61						67		
7		71		73						79
8				83						89
9								97		

Nous ne conserverons, dans ce tableau, que les nombres premiers. Le plus petit d'entre eux est 2 dont nous supprimons tous les multiples. Le suivant est 3; le plus petit des multiples de 3 non déjà supprimé est 9, 6 étant déjà considéré comme multiple de 2. Tous les multiples de 3 sont donc rayés. Le nombre non rayé suivant 3 est 5 qui est premier et dont le plus petit multiple non supprimé est 25 (son carré), les précédents étant déjà supprimés comme multiples de 2 ou 3. Et ainsi de suite. Lorsqu'on arrive à 11, le plus petit multiple non rayé n'appartient pas au tableau. Il en est de même pour tous les nombres figurant dans le tableau, qui suivent 11 et ne sont pas rayés : ils sont donc tous premiers.

Deuxième cas : $100 < n$. Nous nous contenterons d'étudier un exemple.
Soit le nombre $n = 491$. Est-il premier?
D'après le lemme, si n n'est pas premier, il admet au moins un diviseur premier dont le carré lui est inférieur.
Calculons donc les restes des divisions de 491 par les nombres premiers successifs jusqu'à ce que l'on trouve un reste nul ou jusqu'à ce que le carré du diviseur premier considéré dépasse n (auquel cas n sera déclaré premier). Pour chaque diviseur premier p, posons :

$$n = pq + r.$$

On obtient les résultats consignés dans le tableau suivant :

p	q	r	p^2
2	245	1	4
3	163	2	9
5	98	1	25
7	70	1	49
11	44	7	121
13	37	10	169
17	28	15	289
19	25	16	361
23	21	8	529

Le carré de 23 dépasse 491. Il n'existe donc aucun nombre premier dont le carré soit inférieur à 491 et qui divise 491. Ce nombre 491 est donc un nombre premier.

REMARQUE PRATIQUE

En observant le tableau de résultats ci-dessus, nous nous apercevons que : en même temps que le carré de p a dépassé n, on a obtenu $q < p$. Démontrons que la réciproque est vérifiée, c'est-à-dire que si l'on effectue la division euclidienne de n par p et que l'on trouve $q < p$, alors le carré de p dépasse n (cela évitera le calcul de p^2).
Supposons donc $q < p$. Les nombres p et q étant entiers, il en résulte que $q + 1 \leqslant p$ d'où $pq + p \leqslant p^2$.
Or $r < p$, donc
$pq + r < pq + p \leqslant p^2$, et par suite $n < p^2$.

Pratiquement, *on ne calculera pas le carré de p, mais on arrêtera les recherches dès que l'on trouvera* $q < p$.

EXERCICE

Déterminer si les entiers suivants sont premiers :
1 789 , 1 969 , 2 021 , 2 419 , 2 287 , 839 , 911.

2. 18 NOMBRES PREMIERS ET DIVISIBILITÉ. APPLICATION A $\mathbb{Z}/n\mathbb{Z}$

ATTENTION On ne confondra pas le terme « premier » dans les deux locutions

a est un **nombre premier,**
a et b sont **premiers entre eux.**

A cet égard, l'adoption générale du terme « *entiers étrangers* » à la place de « *entiers premiers entre eux* » est hautement souhaitable.

a) Nombres premiers et divisibilité.

Soit p un nombre premier et n un entier quelconque. Si p divise n, $\Delta(n, p) = |p|$; si p ne divise pas n les seuls diviseurs communs à n et p sont 1 et -1; concluons.

Théorème.

Soit p un nombre premier et n un entier non nul quelconques. Les entiers p et n sont premiers entre eux si et seulement si p ne divise pas n.

Soient p et p' deux entiers premiers tels que $|p| \neq |p'|$; p ne divise pas p' et p' ne divise pas p, d'où :

Corollaire 1.

Deux entiers premiers p et p' tels que $|p| \neq |p'|$ sont premiers entre eux.

Soit p un entier premier divisant le produit ab de deux entiers non nuls quelconques.
Ou bien p divise a, ou bien p ne divise pas a; alors dans ce dernier cas il est premier avec a d'où en utilisant le théorème de GAUSS (§ 2.13 c) p divise b.
Par récurrence vous démontrerez facilement que si p premier divise $a_1 a_2 \ldots a_n$ alors p divise au moins un des facteurs a_i $(1 \leqslant i \leqslant n)$ d'où :

Corollaire 2.

Tout nombre premier divisant un produit d'entiers divise au moins un des facteurs du produit.

Si p entier premier divise un produit de nombres premiers $p_1 p_2 \ldots p_n$ d'après le corollaire précédent il divise au moins l'un d'eux soit p_i. Les diviseurs de p_i étant $1, -1, p_i$ et $-p_i$, il en résulte que $|p| = |p_i|$.

Corollaire 3.

Tout nombre premier p divisant un produit de nombres premiers $p_1, p_2, \ldots, p$ est tel qu'il existe un des facteurs p_i vérifiant $|p_i| = |p|$.

b) Retour sur l'anneau $\mathbb{Z}/n\mathbb{Z}$

Nous savons que quel que soit l'*entier naturel* n $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un *anneau commutatif unitaire*.
Si $n = 0$, la relation d'équivalence qui a permis la définition de $\mathbb{Z}/n\mathbb{Z}$ s'écrit

$$x - y \in 0\,\mathbb{Z} = \{0\},$$

c'est-à-dire $x = y$ donc chaque classe $\dot{x}$ contient le seul élément x; vous démontrerez sans peine que les anneaux

$$(\mathbb{Z}/0\,\mathbb{Z}, +, \times) \quad \text{et} \quad (\mathbb{Z}, +, \times)$$

sont isomorphes.
Si $n = 1$, la relation d'équivalence s'écrit $x - y \in 1\,\mathbb{Z} = \mathbb{Z}$ c'est-à-dire $\mathbb{Z}/1\,\mathbb{Z}$ contient une seule classe par exemple $\dot{0}$.

Nous supposerons $n \geqslant 2$. Cherchons les éléments *inversibles* de $\mathbb{Z}/n\mathbb{Z}$. L'entier, modulo n, $\dot{x}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe $x' \in \mathbb{Z}$ tel que

$$\dot{1} = \dot{x}\dot{x}'$$

c'est-à-dire $\quad \dot{1} = \widehat{xx'}$

ou encore $\quad 1 \equiv xx' \pmod{n}$

Donc x est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe x' et n' de $\mathbb{Z}$ tels que

$$1 = xx' + nn'$$

L'égalité de BEZOUT (§ 2.13 b) nous permet d'énoncer.

Lemme.

Dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ $(n \geqslant 2)$ $\dot{x}$ est inversible si et seulement si x et n sont premiers entre eux.

EXERCICES

1. Quels sont les éléments inversibles de $\mathbb{Z}/4\,\mathbb{Z}$, $\mathbb{Z}/12\,\mathbb{Z}$?

2. Démontrer que, dans $\mathbb{Z}/n\mathbb{Z}$ $(n \geqslant 2)$, $\widehat{n-1}$ est toujours inversible.

Si n est **premier**, n et x sont premiers entre eux si et seulement si n ne divise pas x (cf. Théorème sous-paragraphe a) ci-dessus). C'est-à-dire si et seulement si $\dot{x} \neq \dot{0}$ (car si n divise x, il existe $k \in \mathbb{Z}$ tel que $x = kn$ et on a $\dot{x} = \dot{0}$).
Donc si n est *un nombre premier* l'anneau commutatif unitaire $\mathbb{Z}/n\mathbb{Z}$ est tel que tout $\dot{x} \neq \dot{0}$ est inversible, d'autre part il est évident que $\dot{0} \neq \dot{1}$ et par conséquent (cf. § 2.11 b) $\mathbb{Z}/n\mathbb{Z}$ est un corps.
Si n *n'est pas premier*, nous avons les cas suivants :

1. $n = 0$; $\mathbb{Z}/0\,\mathbb{Z}$ est un anneau isomorphe à $(\mathbb{Z}, +, \times)$, donc $\mathbb{Z}/0\,\mathbb{Z}$ n'est pas un corps.

2. $n = 1$; $\mathbb{Z}/1\,\mathbb{Z}$ contient une seule classe $\dot{0}$; ce n'est pas un corps, un corps ayant au moins deux éléments.

3. $n > 2$; il existe alors p et q de $\mathbb{N}$ tels que $n = pq$ avec $1 < p < n$ et $1 < q < n$ donc $\dot{p} \neq \dot{0}, \dot{q} \neq \dot{0}$ et $\dot{p}\dot{q} = \dot{n} = \dot{0}$; donc dans ce cas $\mathbb{Z}/n\mathbb{Z}$ possède des diviseurs de zéro et, par conséquent n'est pas un corps.
Concluons :

Théorème.
L'anneau $\mathbb{Z}/n\mathbb{Z}$ a une structure de corps si et seulement si n est un entier premier.

2. 19 FACTORISATION D'UN ENTIER EN PRODUIT DE FACTEURS PREMIERS. APPLICATIONS

a) Existence de la factorisation.

Soit un nombre entier relatif N ($|\mathrm{N}| \neq 1$ et $\mathrm{N} \neq 0$). Deux cas sont possibles :

- N est premier.
- N est non premier. Il admet donc au moins un diviseur premier p_1 et on peut écrire

$$\mathrm{N} = p_1 q_1, \quad \text{où} \quad 1 < |q_1| < |\mathrm{N}|.$$

A nouveau, deux cas peuvent se présenter :

1. q_1 *est premier*. Alors $\mathrm{N} = p_1 q_1$ est un produit de deux nombres premiers. On dit qu'on a factorisé N en un produit de facteurs premiers.

2. q_1 *est non premier*. Il admet donc au moins un diviseur premier p_2 et $q_1 = p_2 q_2$, soit $\mathrm{N} = p_1 p_2 q_2$ avec $1 < |q_2| < |q_1| < |\mathrm{N}|$. On poursuit le même raisonnement que précédemment.
On obtient ainsi des quotients successifs tels que :

$$1 < \ldots < |q_2| < |q_1| < |\mathrm{N}|.$$

Il y a donc un nombre fini de valeurs possibles pour ces quotients, et par suite, il est certain qu'il existe un rang $k - 1$ tel que q_{k-1} soit premier, égal à p_k. Le nombre N donné peut alors s'écrire :

$$\mathrm{N} = p_1 p_2 \ldots p_k,$$

où $p_1, p_2, \ldots, p_k$ sont des nombres premiers, distincts ou non. Nous pourrons supposer que tous ces nombres p_i $(1 \leqslant i \leqslant k)$ sont *positifs* et écrire :

$$N = \varepsilon\, p_1 p_2 \ldots p_k,$$

où ε prend la valeur $+1$ ou la valeur -1 suivant que N est *positif* ou *négatif*.

b) Unicité de la factorisation.

Il se pourrait que, par un autre procédé, on ait trouvé une autre décomposition de N en produit de facteurs premiers. Démontrons qu'il y a unicité de cette décomposition.
Supposons que :

$$N = \varepsilon\, p_1 p_2 \ldots p_k = \varepsilon'\, p'_1 p'_2 \ldots p'_h,$$

où $p_1, p_2, \ldots, p_k, p'_1, p'_2, \ldots, p'_h$ sont des nombres premiers positifs distincts ou non. $\varepsilon = \varepsilon'$ puisque ce terme ne dépend que du signe de N.
$p_1 \mid N$, donc $p_1 \mid p'_1 p'_2 \ldots p'_h$; p_1 est premier; donc p_1 est égal à l'un des nombres $p'_1, p'_2, \ldots, p'_h$ (§ 2.18, corollaire 3). Par exemple, supposons que $p_1 = p'_1$. Nous pouvons alors écrire :

$$\varepsilon\, p_1 p_2 \ldots p_k = \varepsilon\, p_1 p'_2 \ldots p'_h$$

d'où :

$$p_2 \ldots p_k = p'_2 \ldots p'_h$$

car tout élément non nul est régulier pour la multiplication dans $\mathbb{Z}$.
Ce raisonnement peut être recommencé pour tout nombre p_i $(1 \leqslant i \leqslant k)$, d'où l'on déduit : $\{p_1, p_2, \ldots, p_k\} \subset \{p'_1, p'_2, \ldots, p'_h\}$. Il peut être fait pour tout nombre

$$p'_j \ (1 \leqslant j \leqslant h), \quad \text{d'où}$$
$$\{p'_1, p'_2, \ldots, p'_h\} \subset \{p_1, p_2, \ldots, p_k\}.$$

Par suite : $\{p_1, p_2, \ldots, p_k\} = \{p'_1, p'_2, \ldots, p'_h\}$, ce qui prouve qu'il y a *unicité* de la décomposition de N en produit de facteurs premiers à condition de ne pas avoir égard à l'ordre dans lequel sont écrits les facteurs premiers.
Dans l'étude précédente on ne suppose pas que les facteurs premiers strictement positifs $p_1, p_2, \ldots, p_k$ sont distincts. Pour tout entier relatif N distinct de 0, 1 et -1 nous aurons donc en supposant $p_1, p_2, \ldots, p_n$ tous distincts

$$N = \varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

où $\varepsilon = +1$ ou $\varepsilon = -1$ suivant que $N > 0$ ou $N < 0$ et où $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont des entiers naturels non nuls.

Théorème.

Tout entier relatif non nul et distinct de 1 et -1 peut s'écrire d'une manière unique sous la forme

$$N = \varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

où $\varepsilon = 1$ ou -1, $p_1, p_2, \ldots, p_n$ sont des nombres premiers strictement positifs tous distincts et $\alpha_1, \alpha_2, \ldots, \alpha_n$ des entiers naturels non nuls.

c) Application 1 : recherche des diviseurs et des multiples d'un nombre.

Soit $N = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, d un diviseur de N. Il existe un nombre q tel que : $N = dq$, soit :

$$\varepsilon\, p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} = dq.$$

Les nombres écrits dans chaque membre de cette égalité ayant même factorisation en produit de facteurs premiers, le nombre d est de la forme :

$$d = \varepsilon' p_1^{\delta_1} p_2^{\delta_2} \dots p_n^{\delta_n}$$

avec, pout tout i $(1 \leqslant i \leqslant n)$,

$$0 \leqslant \delta_i \leqslant \alpha_i \quad \text{et} \quad \varepsilon' = +1 \text{ ou } -1$$

Considérons le produit :

$$(p_1^0 + p_1^1 + \dots + p_1^{\alpha_1})(p_2^0 + p_2^1 + \dots + p_2^{\alpha_2}) \dots (p_n^0 + p_n^1 + \dots + p_n^{\alpha_n}).$$

Chaque terme de son développement s'obtient en choisissant un terme dans chaque parenthèse et en faisant le produit de ces termes. Ceci prouve que chaque terme du produit est un nombre

$$d' = p_1^{\delta_1} p_2^{\delta_2} \dots p_n^{\delta_n}$$

avec, pour tout i $(1 \leqslant i \leqslant n)$

$$0 \leqslant \delta_i \leqslant \alpha_i.$$

C'est donc au signe près un diviseur de N, et tous les diviseurs de N s'obtiennent par ce procédé. Il y en a donc : $2(1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_n)$.
(Le 2 vient du choix possible $\varepsilon = +1$ ou $\varepsilon = -1$).

EXEMPLE 1

$N = 120 = 2^3 \times 3 \times 5$. Cherchons ses diviseurs positifs.

$(1 + 2 + 2^2 + 2^3)(1 + 3)(1 + 5) = 1 + 2 + 2^2 + 2^3 + 3 + (2 \times 3) + (2^2 \times 3)$
$+ (2^3 \times 3) + 5 + (2 \times 5) + (2^2 \times 5) + (2^3 \times 5) + (3 \times 5)$
$+ (2 \times 3 \times 5) + (2^2 \times 3 \times 5) + (2^3 \times 3 \times 5)$

L'ensemble des diviseurs positifs de 120 est donc :

$$\{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}.$$

On vérifie que le nombre de diviseurs positifs de 120 est égal à $4 \times 2 \times 2$.

EXERCICE

1. Déterminer le plus petit nombre entier positif qui admet 15 diviseurs positifs.

Soit m un *multiple* de N; il existe un nombre entier k tel que $m = Nk$, c'est-à-dire

$$m = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} k.$$

Il se peut que la décomposition de k contienne certains des facteurs $p_1 \dots p_n$ donc la décomposition de m en facteurs premiers contient tous ces facteurs p_i $(1 \leqslant i \leqslant n)$ avec un exposant $\mu_i \geqslant \alpha_i$; on a donc

$$m = \varepsilon' p_1^{\mu_1} p_2^{\mu_2} \dots p_n^{\mu_n} k'$$

où $\varepsilon' = 1$ ou -1, $k' \in \mathbb{Z}$ et pour tout i $(1 \leqslant i \leqslant n)$

$$\mu_i \geqslant \alpha_i.$$

d) Application 2 : recherche du plus grand diviseur commun à deux nombres a et b.

Soit a et b deux nombres dont on connaît les factorisations en produits de facteurs premiers positifs. Soit $\{p_1, p_2, \dots, p_m\}$ *l'ensemble de tous les facteurs premiers distincts* qui interviennent dans ces *deux* factorisations. On peut poser :

$$a = \varepsilon p_1^{\alpha_1} . p_2^{\alpha_2} \dots p_m^{\alpha_m} \quad \text{avec} \quad \alpha_i \geqslant 0,$$
$$b = \varepsilon' p_1^{\beta_1} . p_2^{\beta_2} \dots p_m^{\beta_m} \quad \text{avec} \quad \beta_i \geqslant 0.$$

On a $\alpha_i \geqslant 0$ (et non $\alpha_i > 0$) car si p_i ne figure pas dans la factorisation de a on a $\alpha_i = 0$, de même pour β_i.

Soit d un diviseur commun à a et b. D'après les résultats du paragraphe précédent on a

$$d = \varepsilon'' p_1^{\delta_1} . p_2^{\delta_2} \ldots p_m^{\delta_m}$$

avec, pour tout i $(1 \leqslant i \leqslant m)$

$$0 \leqslant \delta_i \leqslant \alpha_i \quad \text{et} \quad 0 \leqslant \delta_i \leqslant \beta_i,$$

c'est-à-dire :

$$0 \leqslant \delta_i \leqslant \inf(\alpha_i, \beta_i).$$

Le plus grand diviseur commun de a et b est donc :

$$\Delta = p_1^{\delta'_1} . p_2^{\delta'_2} \ldots p_m^{\delta'_m}$$

avec, quel que soit i $(1 \leqslant i \leqslant m)$

$$\delta'_i = \inf(\alpha_i, \beta_i).$$

EXEMPLE 2

$$360 = 2^3 \times 3^3 \times 5^1 = 2^3 \times 3^3 \times 5^1 \times 7^0$$
$$21 = \quad 3^1 \times 7^1 = 2^0 \times 3^1 \times 5^0 \times 7^1$$
$$\Delta(360, 21) = 2^0 \times 3^1 \times 5^0 \times 7^0 = 3.$$

EXERCICE 1

Déterminer $\Delta(450, 735)$.
Déterminer $\Delta(75, 125, 725)$.

e) **Application 3 : recherche du plus petit multiple commun à deux nombres a et b.**

Soit a et b deux nombres dont on connaît les factorisations en produits de facteurs premiers positifs. Soit $\{p_1, p_2, \ldots, p_m\}$ l'ensemble des nombres premiers distincts qui interviennent dans ces deux décompositions. Comme précédemment, nous pouvons poser :

$$a = \varepsilon\, p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_m^{\alpha_m} \quad \text{avec} \quad \alpha_i \geqslant 0,$$
$$b = \varepsilon'\, p_1^{\beta_1} . p_2^{\beta_2} \ldots p_m^{\beta_m} \quad \text{avec} \quad \beta_i \geqslant 0.$$

Soit m un multiple commun à a et b. Il s'écrit :

$$m = \varepsilon''\, p_1^{\mu_1} . p_2^{\mu_2} \ldots p_m^{\mu_m}$$

avec, quel que soit i $(1 \leqslant i \leqslant m)$, $\mu_i \geqslant \alpha_i$ et $\mu_i \geqslant \beta_i$, soit $\mu_i \geqslant \sup(\alpha_i, \beta_i)$.

Le plus petit multiple commun à a et b est donc égal à :

$$M = p_1^{\mu'_1} . p_2^{\mu'_2} \ldots p_m^{\mu'_m}$$

avec, quel que soit i $(1 \leqslant i \leqslant m)$, $\mu'_i = \sup(\alpha_i, \beta_i)$.

EXEMPLE 3

$$360 = 2^3 \times 3^3 \times 5^1 = 2^3 \times 3^3 \times 5^1 \times 7^0$$
$$21 = 3^1 \times 7^1 = 2^0 \times 3^1 \times 5^0 \times 7^1$$
$$M(360, 21) = 2^3 \times 3^3 \times 5^1 \times 7^1 = 2\,520.$$

EXERCICE 3

Déterminer M (450, 735).
Déterminer M (75, 125, 725).

EXERCICES

Exercices de révision sur les lois internes : 1 à 12; 16, 17; 74, 75.
Homomorphismes et isomorphismes : 12 à 15, 18.
Congruences modulo n : 19 à 34.
Division euclidienne et numération décimale : 35.
P.G.C.D. : 36 à 39; 74.
Théorème de Gauss : 40 à 44; 50 à 52.
Nombres premiers entre eux : 45 à 47.
P.P.C.M. : 51 à 59; 74.
Nombres premiers : 60 à 71.
Problèmes de récapitulation : 49; 71, 72, 73; 76.

2.1 Soit E un ensemble, A une partie propre de E; on désigne par $\mathcal{A}_1$ l'ensemble des parties X_1 de E telles que $A \subset X_1$ et par $\mathcal{A}_2$ l'ensemble des parties X_2 de E telles que $X_2 \subset A$.

a) Démontrer que $\mathcal{A}_1$ et $\mathcal{A}_2$ sont des parties stables de E pour la réunion et pour l'intersection.

b) Les trois ensembles $\mathcal{P}(E)$, $\mathcal{A}_1$ et $\mathcal{A}_2$ ont-ils chacun un élément neutre pour la réunion? ces éléments neutres sont-ils les mêmes?

c) Mêmes questions qu'en *b*, mais pour l'intersection.

2.2 On munit l'ensemble $E = \mathbb{Z} \times \mathbb{Z}$ de la multiplication définie quels que soient a, a', b, b' de $\mathbb{Z}$ par

$$(a, a')(b, b') = (ab, a'b').$$

a) Démontrer que la multiplication dans E est associative, commutative et possède un élément neutre e.

b) Caractériser tous les éléments réguliers de $(E, \times)$.

c) Démontrer que $A = \mathbb{Z} \times \{0\}$ est une partie stable de $(E, \times)$. Quel est l'élément neutre ε de $(A, \times)$?

2.3 Soit A une partie stable de $(E, \star)$. On suppose que $(E, \star)$ a un élément neutre e.

a) Démontrer que si $e \in A$, alors e est élément neutre de $(A, \star)$.

b) Si $e \notin A$ donner des exemples où $(A, \star)$ n'a pas d'élément neutre et des exemples où $(A, \star)$ a un élément neutre ε.

2.4 On munit l'ensemble des applications de $\mathbb{R}$ dans $\mathbb{R}$, c'est-à-dire $E = \mathcal{F}(\mathbb{R}, \mathbb{R})$, soit de la *multiplication* des fonctions numériques soit de la *composition* des fonctions numériques.

a) Quel est l'élément neutre de E pour chacune de ces lois?

b) Quels sont les éléments symétrisables de $(E, \times)$? de (E, o)? Y-a-t-il dans E des éléments symétrisables à la fois pour la multiplication et la composition?

2.5 Soit $(G, +)$ un groupe d'élément neutre e. Pour tout a de G et tout n de $\mathbb{Z}$ on pose

$$\begin{aligned} na &= a + a + \ldots + a \qquad (n \text{ termes}) \quad \text{si} \quad 0 < n, \\ 0a &= e, \\ na &= (-n)(-a) \qquad \text{si} \quad n < 0. \end{aligned}$$

On désigne par A l'ensemble de tous les éléments de la forme na ($a \in G$ fixé, n entier relatif quelconque).

a) Démontrer que A est un sous-groupe de G; on dit que A est le sous-groupe engendré par a.

b) On suppose G fini et on considère a de G. Démontrer qu'il existe au moins un entier $q > 0$ tel que $qa = e$. Le plus petit des entiers q, soit p, est appelé l'*ordre* de l'élément a; démontrer que p est le nombre des éléments du sous-groupe engendré par a.

c) Trouver l'ordre de chacun des éléments de $(\mathbb{Z}/12\,\mathbb{Z}, +)$.

2.6 Soit $(G, \times)$ un groupe d'élément neutre e. Pour tout a de G et tout n de $\mathbb{Z}$ on pose

$$a^n = a \times a \times \ldots \times a \quad (n \text{ facteurs}) \quad \text{si} \quad 0 < n,$$
$$a^0 = e,$$
$$a^n = (a^{-1})^{-n} \quad \text{si} \quad n < 0.$$

On désigne par A l'ensemble de tous les éléments de la forme a^n ($a \in G$ fixé, n entier relatif quelconque).

a) Démontrer que A est un sous-groupe de G; on dit que A est le *sous-groupe engendré* par a.

b) On suppose G fini et on considère $a \in G$. Démontrer qu'il existe au moins un entier $q > 0$ tel que $a^q = e$. Le plus petit des entiers q, soit p, est appelé l'*ordre* de l'élément a : démontrer que p est le nombre d'éléments du sous-groupe engendré par a.

c) On pose $G = \mathbb{Z}/11\,\mathbb{Z} - \{\dot{0}\}$. Vérifier que $(G, \times)$ est un groupe; trouver l'ordre de chacun de ses éléments.

2.7 Soit $(A, +, \times)$ un anneau unitaire. On désigne par U l'ensemble des éléments inversibles de A.

a) Démontrer que $(U, \times)$ est un groupe. Quel est le groupe U si A est un corps?

b) Quel est le groupe U de l'anneau $\mathbb{Z}$? de l'anneau $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times)$? de l'anneau $\mathbb{Z}/12\,\mathbb{Z}$?

2.8 Soit A un anneau commutatif, unitaire, sans diviseurs de zéro, fini de cardinal $n \geqslant 2$. On désigne par ω l'élément zéro, par e l'élément unité et on pose $A^* = A - \{\omega\}$.

a) Démontrer que $\omega \neq e$.

b) Démontrer que, quel que soit a de A^*, l'application de A^* dans A^* défini par $x \longmapsto ax$ est injective.
En déduire qu'elle est bijective (A^* est fini). Conclure : A est un corps.

c) Démontrer que l'anneau $\mathbb{Z}/n\,\mathbb{Z}$ est un corps si et seulement si n est un nombre premier.

2.9 Soit X un ensemble quelconque; on considère l'anneau $A = (\mathcal{F}(X, \mathbb{R}), +, \times)$.
Démontrer qu'il y a dans A des diviseurs de zéro (on pourra considérer deux parties propres X_1 et X_2 complémentaires dans X). Expliciter des fonctions f et g telles que $fg = 0_A$ lorsque X est un intervalle $[a, b]$ de $\mathbb{R}$ ($a < b$).

2.10 On munit $E = \mathbb{Z} \times \mathbb{Z}$ d'une addition et d'une multiplication définies quels que soient a, a', b, b' de $\mathbb{Z}$ par :

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a')\,(b, b') = (ab, a'b').$$

a) Démontrer que $(E, +, \times)$ est un anneau commutatif.

b) Déterminer tous les diviseurs de zéro de cet anneau.

2.11 On munit $E = \mathbb{Z} \times \mathbb{Z}$ d'une addition et d'une loi interne notée $\star$ définies quels que soient a, a', b, b' de $\mathbb{Z}$ par :

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a') \star (b, b') = (ab, o).$$

a) Démontrer que $(E, +, \star)$ est un anneau commutatif.

b) Démontrer que tout élément de E est un diviseur de zéro.

c) Existe-t-il des éléments réguliers pour la loi $\star$?

d) Étudier les solutions de l'équation :

$$(a, a') \star (x, x') = (b, b')$$

où (a, a') et (b, b') sont des éléments donnés de E et (x, x') un élément inconnu de E.

2.12 On considère $K = \{e, a, b, c\}$ muni de la multiplication où e est élément neutre et définie, de plus, par $a^2 = b^2 = c^2 = e$, $bc = cb = a$, $ca = ac = b$, $ab = ba = c$.
Dans le plan euclidien E_2 on considère un repère orthonormé d'axes Ox et Oy et les trois symétries s_x d'axe Ox, s_y d'axe Oy et s_0 de centre O; on pose de plus $e' = \mathrm{Id}_{E_2}$ et $K' = \{e', s_x, s_y, s_0\}$.

a) Démontrer que (K′, o) est un groupe.
b) Démontrer que l'application f de K dans K′ définie par $f(e) = e'$, $f(a) = s_x$, $f(b) = s_y$, $f(c) = s_0$ est un isomorphisme de (K, ×) sur (K′, o).
En déduire que K est un groupe; il est appelé groupe de KLEIN.
c) On munit $E = (\mathbb{Z}/2\,\mathbb{Z}) \times (\mathbb{Z}/2\,\mathbb{Z})$ de l'addition définie par :

$$(\dot{a}, \dot{a}') + (\dot{b}, \dot{b}') = (\dot{a} + \dot{b}, \dot{a}' + \dot{b}')$$

Déterminer tous les éléments de E et la table de (E, +). Démontrer que (E, +) est un groupe isomorphe au groupe de KLEIN.

2.13 Soit f un homomorphisme du groupe $(\mathbb{Z}, +)$ dans lui-même.
a) Démontrer que pour tout n de $\mathbb{N}$, $f(n) = nf(1)$ (raisonner par récurrence).
En déduire que f est déterminée par la valeur $f(1) = a \in \mathbb{Z}$.
b) Démontrer que si $a \neq 0$, f est un homomorphisme injectif. Dans quel cas est-il surjectif? Trouver tous les isomorphismes de $(\mathbb{Z}, +)$ sur lui-même.

2.14 Soit f un homomorphisme de l'anneau $(\mathbb{Z}, +, \times)$ dans lui-même.
Démontrer que, s'il existe $x_0 \in \mathbb{Z}$ tel que $f(x_0) \neq 0$, on a $f(1) = 1$.
En déduire que f est soit l'application nulle, soit l'application identique (utiliser ex. 2.13).

2.15* On considère le groupe additif $G = \mathbb{Z}/n\mathbb{Z}$.
a) Démontrer qu'un homomorphisme de (G, +) dans lui-même est déterminé par $f(\dot{1})$. Combien y a-t-il d'homomorphismes de (G, +) dans lui-même?
b) Comment faut-il choisir l'entier a dans $[0\,,\, n-1]$ pour que f défini par $f(\dot{1}) = \dot{a}$ soit un isomorphisme?

2.16 Soit (G, +) un groupe commutatif et P une partie stable de G telle que $P \cap (-P) = \{e\}$ (e est l'élément neutre de G, $-P$ l'ensemble des opposés des éléments de P).
a) Démontrer que la relation $y - x \in P$ est une relation d'ordre définie sur G et que cette relation est compatible avec l'addition.
b) Démontrer que cette relation définit un ordre total si et seulement si $G = P \cup (-P)$.

2.17 Soit G un groupe; on appelle *centre* C de G l'ensemble des éléments de G qui permutent avec tout élément de G. Donc $a \in C$ si et seulement si

$$(\forall\, x \in G) \quad ax = xa.$$

a) C peut-il être vide? Peut-on avoir $C = G$?
b) Démontrer que C est un sous-groupe du groupe G.

2.18* Soit G un groupe noté multiplicativement, e son élément neutre et C son centre (cf. ex. 2.17). On suppose G non commutatif. A tout élément a de G on associe l'application f_a de G dans G définie, pour tout x de G, par $f_a(x) = axa^{-1}$. On désigne enfin par G′ l'ensemble de toutes les applications f_a, a étant un élément quelconque de G.
a) Démontrer que f_a est un isomorphisme du groupe G sur lui-même.
b) Démontrer que (G′, o) est un groupe. On déterminera successivement $f_a \circ f_b$, f_e, $(f_a)^{-1}$.
c) Démontrer que l'application

$$\varphi : G \longrightarrow G', \qquad a \longmapsto f_a$$

définit un homomorphisme surjectif du groupe (G, ×) sur le groupe (G′, o).
d) Démontrer que φ est un isomorphisme si et seulement si $C = \{e\}$.

2.19 Résoudre dans $\mathbb{Z}/7\,\mathbb{Z}$: $x^2 + x + \dot{1} = \dot{0}$.
Résoudre dans $\mathbb{Z}/6\,\mathbb{Z}$: $x^2 + x + \dot{1} = \dot{0}$.
Résoudre dans $\mathbb{Z}/7\,\mathbb{Z}$:
$$\begin{cases} x + y = \dot{3}, \\ x - y = \dot{5}. \end{cases}$$
Résoudre dans $\mathbb{Z}/5\,\mathbb{Z}$:
$$\begin{cases} \dot{2}x + \dot{3}y = \dot{1}, \\ x - \dot{2}y = \dot{3}. \end{cases}$$

2.20 Démontrer que, pour tout nombre entier naturel n :

$$n^3 \text{ est de la forme } 7k,\ 7k+1 \quad \text{ou} \quad 7k-1.$$

2.21 Calculer $(\dot{x})^n$ pour chacun des éléments de $\mathbb{Z}/7\,\mathbb{Z} - \{\dot{0}\}$. Pour chacun de ces éléments on trouvera un entier p, dépendant de l'élément $\dot{x}$ choisi tel que $1 \leqslant p \leqslant 6$ et $(\dot{x})^p = \dot{1}$. Expliquer le résultat obtenu en considérant le groupe multiplicatif $\mathbb{Z}/7\,\mathbb{Z} - \{\dot{0}\}$ (cf. ex. 2.6).

Application : Trouver le reste de la division euclidienne de 1971^{1000} par 7.

2.22 Étudier les restes de la division par 7 des nombres 2^n et 3^n (n est un entier naturel).
Résoudre alors l'équation :

$$2^x + 3^x \equiv 0 \pmod 7,$$

où x désigne un entier positif.

2.23 Calculer le reste de la division euclidienne de l'entier naturel

$$n = 19^{52} \times 23^{41}$$

par 7.

2.24 Étudier les restes des divisions par 9 des différentes puissances de 2. Montrer que le nombre

$$E = 2^{2n}(2^{2n+1} - 1) - 1,$$

où n désigne un entier naturel, est toujours divisible par 9.

2.25 Soit n un entier positif. Quel est le reste de la division par 4 de la somme

$$1^n + 2^n + 3^n + 4^n ?$$

2.26 Démontrer que, quel que soit l'entier $n \geqslant 1$, l'entier $A = n^3(n^2 - 1)$ est divisible par 12.

2.27 Démontrer que, pour tout entier naturel n, on a

$$3^{3n+2} + 2^{n+4} \equiv 0 \pmod 5.$$

2.28 Démontrer les propriétés suivantes, valables quel que soit l'entier naturel n :
(1) $3^{2n} - 2^n$ est divisible par 7;
(2) $n_4^{n+1} - (n+1)4^n + 1$ est divisible par 9;
(3) $4^n + 6n - 1$ est divisible par 9;
(4) $3 \times 5^{2n-1} + 2^{3n-2}$ est divisible par 17;
(5) $3^{2n+1} + 2^{n+2}$ est divisible par 7;
(6) $3^{2n} + 2^{6n-5}$ est divisible par 11;
(7) $(a+1)^{n+1} - a(n+1) - 1$ est divisible par a^2
(a est un nombre entier naturel quelconque).

2.29 Déterminer les nombres entiers n tels que $n^5 - 2$ soit divisible par 7.

2.30 Déterminer les entiers relatifs n tels que

$$n^2 - 3n + 6 \equiv 0 \pmod 5.$$

2.31 Déterminer les entiers naturels n tels que le nombre N défini par

$$N = n^3 + n - 2$$

soit divisible par 7.

2.32 A quelle condition le nombre $N = 2^{2n} + 2^n + 1$ (où n est un nombre entier naturel) est-il divisible par 7?

2.33 Trouver un nombre entier relatif n tel que :

$$n^2 + n + 7 \equiv 0 \pmod{13}.$$

En déduire l'ensemble des entiers relatifs satisfaisant à cette condition.

2.34 On considère le nombre

$$N = (n-1)n + n(n+1) + (n-1)(n+1),$$

où n est un entier supérieur à 2.
Démontrer que ce nombre n'est divisible ni par 3, ni par 5, ni par 7.

2.35 Déterminer un nombre n de quatre chiffres, dans le système de base dix, tel que les restes des divisions de 21 685 et 33 509 par n soient respectivement 37 et 53.

2.36 Déterminer les nombres entiers naturels tels que

$$\begin{cases} a + b = 182, \\ \Delta(a, b) = 13. \end{cases}$$

2.37 Soit deux entiers quelconques a et b. On considère les deux nombres A et B tels que

$$A = 5a + 4b \quad \text{et} \quad B = 11a + 9b.$$

Démontrer que

$$\Delta(a, b) = \Delta(A, B).$$

On généralise ce résultat : on considère les deux nombres A′ et B′ tels que

$$A' = pa + qb \quad \text{et} \quad B' = ra + sb \quad \text{avec} \quad ps - qr = 1.$$

Démontrer que

$$\Delta(a, b) = \Delta(A', B').$$

2.38 Calculer le plus grand diviseur commun des nombres

$$5\,145 \quad , \quad 4\,410 \quad , \quad 3\,675.$$

Résoudre l'équation

$$3\,675\,x - 5\,145\,y = 4\,410,$$

où x et y appartiennent à $\mathbb{N}$, ensemble des entiers naturels.
(On remarquera que (4, 2) est une solution particulière de l'équation.)

2.39 Soit les nombres entiers naturels a, b, c, d tels que $a > b > c > d$.
1° Montrer que, dans la recherche du plus grand diviseur commun de ces nombres, on peut remplacer a, b, c par les restes respectifs de leurs divisions par d.
2° Appliquer cette propriété autant de fois qu'il le faudra pour trouver le plus grand diviseur commun aux nombres :

$$58\,212 \quad , \quad 24\,948 \quad , \quad 21\,924 \quad , \quad 13\,608.$$

2.40 Déterminer les couples (x, y) d'entiers relatifs solutions de l'équation :

$$x^2 - y^2 = 1\,969.$$

2.41 Soit x et y appartenant à $\mathbb{N}$, ensemble des entiers naturels. Résoudre l'équation

$$9y^2 - (x + 1)^2 = 32.$$

2.42 Trouver tous les couples d'entiers relatifs (x, y) solution de

$$11x - 5y = 14,$$

sachant que (19, 39) est une solution particulière.
Montrer qu'il existe un couple et un seul (x_0, y_0) solution de cette équation avec

$$0 \leqslant x_0 < 5.$$

2.43 Déterminer tous les couples (x, y) d'entiers relatifs tels que

$$65x = 16y.$$

Sachant que le couple (1, 4) est solution de l'équation

$$65x - 16y = 1,$$

déterminer tous les couples (x, y) d'entiers relatifs tels que

$$65x - 16y = 7.$$

2.44 Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ l'équation

$$151x - 77y = 1.$$

En déduire la résolution, dans $\mathbb{Z} \times \mathbb{Z}$ de

$$151x - 77y = 5.$$

2.45 Démontrer que $n^7 - n$ est divisible par 42, quel que soit n entier supérieur à 1.

2.46 Démontrer que le nombre 28 710 est divisible par 495, sans effectuer la division. Démontrer, de même, que le nombre 73 260 est divisible par 1980.

2.47 Démontrer que, quel que soit l'entier naturel n,

(1) $n^3 - n$ est divisible par 6;
(2) $n^5 - n$ est divisible par 30;
(3) $n^7 - n$ est divisible par 42;
(4) $n^3 + 11\,n$ est divisible par 6;
(5) $n\,(n^2 - 1)\,(n^2 + 1)$ est divisible par 60;
(7) $n\,(n + 1)\,(2\,n + 1)$ est divisible par 6;
(8) $n\,(2\,n + 1)\,(7\,n + 1)$ est divisible par 6;
(9) $n\,(n + 1)\,(n + 2)\,(n + 3)$ est divisible par 24;
(10) $n\,(n + 1)\,(n + 2)\,(n + 3)\,(n + 4)$ est divisible par 120.

2.48 Résoudre les congruences suivantes, où n désigne un entier relatif

(1) $n + 8 \equiv 0 \pmod{n - 2}$,
(2) $n + 7 \equiv 0 \pmod{n - 5}$,
(3) $3\,n - 27 \equiv 0 \pmod{n + 3}$.

2.49 Le nombre n est un entier naturel donné. Les lettres x et y désignent des entiers supérieurs à $2\,n$ vérifiant

$$(x - 2\,n)\,(y - 2\,n) = 2\,n^2 \qquad (1)$$

1° Démontrer que tout diviseur commun à $x - 2\,n$ et $y - 2\,n$ divise x et y.
2° En montrant que (1) se met sous la forme

$$x^2 + y^2 = (x + y - 2\,n)^2,$$

montrer que tout diviseur commun à x et y divise $x - 2\,n$ et $y - 2\,n$.
3° Démontrer que tout diviseur commun à x et y divise n.
4° On suppose $n = 30$. Trouver tous les couples (x, y) premiers entre eux vérifiant la relation (1).

2.50 On donne un nombre entier a ($a \geqslant 2$) et deux nombres entiers positifs m et n ($m > n$). On suppose que l'on a

$$m = nq + r \qquad 0 < r < n.$$

On pose

$$\mathrm{M} = a^m - 1 \quad , \quad \mathrm{N} = a^n - 1 \quad , \quad \mathrm{R} = a^r - 1.$$

On sait que $\Delta\,(m, n) = \Delta\,(n, r)$. A-t-on $\Delta\,(\mathrm{M}, \mathrm{N}) = \Delta\,(\mathrm{N}, \mathrm{R})$?
Déterminer $\Delta\,(\mathrm{M}, \mathrm{N})$.
Application

$$\mathrm{M} = 99\ldots\ldots9 \quad (\mathrm{M}\text{ a 4 679 chiffres}),$$
$$\mathrm{N} = 99\ldots\ldots9 \quad (\mathrm{N}\text{ a 2 519 chiffres}).$$

Calculer $\Delta\,(\mathrm{M}, \mathrm{N})$.

2.51 Le nombre n est un entier naturel, supérieur ou égal à 2.
Démontrer que $C_n^2 + 1$ n'est pas divisible par 3.
Démontrer que le nombre : $C_{C_n^2}^2$ est divisible par 3.

2.52 Le nombre n est un entier relatif non nul et différent de 1.
Calculer

$$\Delta\,(n, n + 1), \quad \mathrm{M}\,(n, n + 1), \quad \Delta\,(n, 2\,n + 1), \quad \mathrm{M}\,(n, 2\,n + 1),$$
$$\Delta\,(n, n + 1, 2\,n + 1), \quad \mathrm{M}\,(n, n + 1, 2\,n + 1),$$
$$\Delta\,(n - 1, n, n + 1), \quad \mathrm{M}\,(n - 1, n, n + 1).$$

2.53 Déterminer tous les couples de nombres entiers naturels tels que

$$a \times b = 12\,950$$
$$\mathrm{M}(a, b) = 2\,590$$

2.54 Démontrer que, quels que soient a et b, entiers naturels, les propriétés suivantes sont équivalentes :

1. a et b sont des multiples de 7;
2. $a^2 + b^2$ est divisible par 7.

2.55 Déterminer tous les couples d'entiers naturels admettant 36 pour plus grand diviseur commun et 7 560 pour plus petit multiple commun.

2.56 Étant donné un entier naturel n, on considère les deux nombres a et b tels que

$$a = 2n^2 \quad \text{et} \quad b = n(2n + 1).$$

On pose

$$d = \Delta(a, b) \quad \text{et} \quad m = \mathrm{M}(a, b).$$

Démontrer que l'on a

$$b - a = d \quad \text{et} \quad b^2 - a^2 = m - d^2.$$

2.57 Soit trois nombres entiers naturels x, y, z. Soit $\mu = \mathrm{M}(x, y, z)$.

1° Soit $\delta = \Delta(yz, zx, xy)$. Démontrer que : $\delta\mu = xyz$.

2° Soit $m = \mathrm{M}(x, y)$, $m' = \mathrm{M}(x, z)$. Démontrer que $\mu = \mathrm{M}(m, m')$.

3° Application

$$x = 120 \quad , \quad y = 65 \quad , \quad z = 210.$$

2.58 Soit trois nombres entiers naturels x, y, z.

On pose

$$a = \Delta(y, z) \quad , \quad b = \Delta(x, z) \quad , \quad c = \Delta(x, y),$$
$$a' = \mathrm{M}(y, z) \quad , \quad b' = \mathrm{M}(x, z) \quad , \quad c' = \mathrm{M}(x, y).$$

Démontrer que

$$\Delta(xy, yz, zx) = \Delta(ax, by, cz),$$

et

$$\mathrm{M}(xy, yz, zx) = \mathrm{M}(a'x, b'y, c'z).$$

2.59 On marque n points équidistants sur un cercle. On les joint de p en p. On obtient un polygone régulier (en général).

Étudier la nature du polygone obtenu (convexe ou croisé) et le nombre de ses côtés.

2.60 Décomposer en produit de nombres premiers les nombres suivants :

$$720 \; ; \; 2\,860 \; ; \; 8\,040 \; ; \; 1\,323.$$

2.61* Démontrer qu'un nombre entier est un carré parfait si, et seulement si, il admet un nombre impair de diviseurs positifs.

2.62 Déterminer les expressions générales de la décomposition en produit de nombres premiers des entiers naturels qui ont 24 diviseurs positifs. Quel est le plus petit d'entre eux?

2.63 On considère le nombre $\mathrm{E} = n^4 + n^2 + 1$, n étant un entier positif et non nul.

1° Décomposer E en produit de deux facteurs du second degré et démontrer que ces deux facteurs sont premiers entre eux.

2° Le nombre E peut-il être premier?

2.64 Combien de fois le nombre 2 intervient-il dans la décomposition de 100! en produit de nombres premiers?

65 Soit n un entier naturel différent de 0 et de 1.
On considère les $n - 1$ nombres :

$$n! + 2, \quad n! + 3, \quad \ldots, \quad n! + (n-1), \quad n! + n.$$

Démontrer que ces nombres ne sont pas premiers.
En déduire que l'on peut trouver une suite de k nombres consécutifs non premiers. Application : $k = 100$.

2.66 Théorème de FERMAT :
1° Soit p et n deux entiers naturels, avec p premier et $\Delta(n, p) = 1$. On considère les nombres :

$$n, \quad 2n, \quad 3n, \quad \ldots, \quad (p-1)n.$$

Démontrer que, si on les divise par p, on obtient des restes tous différents et non nuls.
En déduire que

$$n^{p-1} \equiv 1 \pmod{p}.$$

2° Démontrer que, pour tout nombre p premier et pour tout nombre entier naturel non nul a,

$$a^p \equiv a \pmod{p}.$$

(cf. ex. 2.76)

2.67 1° Déterminer l'ensemble des diviseurs du nombre 300.
2° Donner une forme caractéristique d'un couple d'entiers strictement positifs ayant pour plus grand diviseur commun leur différence.
3° Trouver tous les couples d'entiers qui ont pour plus grand diviseur commun leur différence et pour plus petit multiple commun 300.

2.68 1° Démontrer que, si n est premier, quel que soit p $(0 < p < n)$, C_n^p est divisible par n.
2° Réciproquement, on suppose que : quel que soit p $(0 < p < n)$, C_n^p est divisible par n.
On se propose de démontrer que n est premier. On supposera que n n'est pas premier, donc qu'il existe deux entiers r et s tels que $n = rs$ avec r premier. En calculant C_n^r, on montrera que l'hypothèse faite est impossible et que, par suite, n est premier.

2.69 Les lettres n, n', p, p' désignent des entiers naturels.
1° On suppose que

$$p = n^4 + 4.$$

Déterminer n tel que p soit premier.
2° Les deux nombres n et n' sont tels que : $|n - n'| = 2$.
D'autre part

$$p = n^4 + 4 \quad , \quad p' = n'^4 + 4.$$

Démontrer que p et p' ne sont pas premiers entre eux.

2.70* Dans cet exercice, on ne considérera que des nombres entiers naturels. On s'intéresse aux nombres inférieurs à un nombre entier donné n et qui sont premiers avec n. On désigne par $\varphi(n)$ leur nombre.
Par exemple : $\varphi(8) = 4$.
1° On suppose que la décomposition de n en produit de nombres premiers s'écrit :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}.$$

Démontrer qu'un nombre est premier avec n si, et seulement si, il n'est multiple ni de p_1, ni de p_2, ni de p_3.
Déterminer l'ensemble des nombres inférieurs à 120 et qui sont premiers avec 120, et en déduire $\varphi(120)$.
2° Démontrer que, plus généralement :

$$\varphi(p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}) = p_1^{\alpha_1 - 1} . p_2^{\alpha_2 - 1} p_3^{\alpha_3 - 1} (p_1 - 1)(p_2 - 1)(p_3 - 1).$$

Démontrer que, si les nombres n et n' sont premiers entre eux

$$\varphi(n) . \varphi(n') = \varphi(nn').$$

2.71 Soit n un nombre entier donné. On désigne par S la suite d'entiers naturels $(1, 2, 3, \ldots, (n-1), n)$. Soit a un nombre premier inférieur ou égal à n.

1° Déterminer, en fonction de n et a, le nombre q_1 des termes de S qui sont des multiples de a. Comment obtient-on à partir de q_1 et de a le nombre q_2 des termes de S qui sont des multiples de a^2?

2° D'une façon générale, q_k étant le nombre des termes de S qui sont multiples de a^k, déterminer, en fonction de q_k et de a, le nombre q_{k+1} des termes de S qui sont multiples de a^{k+1}.

3° On considère le produit : $1.2.3. \ldots (n-1).n = n!$ Soit a un des facteurs premiers figurant dans la décomposition de $n!$ en facteurs premiers. Déterminer l'exposant de a dans cette décomposition, en fonction de $q_1, q_2, \ldots, q_k, \ldots, q_N$ (N étant le plus grand entier vérifiant $a^N \leqslant n$).

4° Application : décomposer 50! en facteurs premiers.

Sujets d'étude.

2.72 Notations. — Toutes les lettres représentent des entiers naturels. ab désigne un produit; $\overline{ab}$ figure l'entier $ax + b$, de chiffres a et b, dans le système de numération de base x; si x dépasse dix, les premiers chiffres après 9 sont notés α (dix), β (onze), γ, δ, ε, ζ (quinze),...

24 (vingt-quatre), sans trait, indique l'emploi de la base dix.

Définition. — Soit n un entier, qui s'écrit $n = \overline{ab}$ dans la base x; on suppose $x \geqslant 3$, $b > a \geqslant 1$; on forme l'entier $n' = \overline{ba}$ (base x); si n divise n', on dira que n est un codiviseur pour la base x. Ainsi, sont des codiviseurs, respectivement :

$n = 12$ pour la base sept : $n = \overline{15}$, $n' = \overline{51}$, $n' = 3n$;

$n = 96$ pour la base dix-sept : $n = \overline{5\beta}$, $n' = \overline{\beta 5}$, $n' = 2n$.

Problème. — 1° On donne une base x et un codiviseur, $n = \overline{ab}$, pour cette base. Il existe, par définition, un entier k tel que

$$\overline{ba} = \overline{ab} \times k \quad \text{(base } x\text{)};$$

montrer que k vérifie les inégalités : $2 \leqslant k \leqslant x - 1$.

Montrer qu'il existe un entier r tel que : $bk = rx + a$, et que r vérifie les inégalités

$$1 \leqslant r \leqslant k - 1.$$

Établir les formules

$$(1) \qquad b = ak + r \quad , \quad x = (k^2 - 1)\frac{a}{r} + k.$$

2° On donne trois entiers, a, k et r, satisfaisant aux conditions

$$(2) \qquad a \geqslant 1 \quad , \quad k \geqslant 2 \quad , \quad 1 \leqslant r \leqslant k - 1;$$

r divise $(k^2 - 1)a$; les formules (1) leur associent deux entiers, b et x; a et b sont-ils les chiffres, dans la base x, d'un codiviseur pour cette base?

3° On donne $a \geqslant 1$ et $k \geqslant 2$. La valeur $r_1 = k - 1$ de r vérifie (2); soit x_1 la base associée; écrire $x_1 + 1$ sous forme de produit.

Si une autre valeur, r_2, de r vérifie (2) et si x_2 est la base associée, montrer qu'on a $x_2 > x_1$ et que $x_2 + 1$ n'est pas premier avec $k + 1$. Choisir a_0, k_0, r_0 pour rendre minimale la base x_0 associée.

4° La donnée est désormais celle d'une base x $(x \geqslant x_0)$.

Dans le cas où $x + 1 = uv$, $u \geqslant 3$, $v \geqslant 2$, mettre en évidence un codiviseur pour la base x et l'évaluer au moyen de u et v.

Exprimer, par une propriété caractéristique de $x + 1$, qu'il n'existe aucun codiviseur pour une base donnée x.

Trouver tous les codiviseurs pour la base $x = 17$ (les résultats acquis permettent une recherche méthodique et rapide). Pourquoi 16 divise-t-il trois des codiviseurs obtenus?

2.73 Dans le système de numération de base x, on se propose de trouver facilement le reste de la division d'un nombre N par un nombre a donné. On étudiera chacun des cas suivants :

1° $a = x^p$ $(p \in \mathbb{N}^*)$.

2° $a = x - 1$ (on remarquera que $x \equiv 1 \pmod{x - 1}$).

3° $a = x + 1$.

4° a est un diviseur de x.

5° a est un diviseur de $x - 1$, ou de $x + 1$.

6° Application : trouver une condition nécessaire et suffisante pour qu'un nombre N donné en base dix soit divisible par a

$$a \in \{10^3,\ 2,\ 5,\ 9,\ 11,\ 3\}.$$

Déterminer les chiffres x, y, z du nombre $N = \overline{z\,17\,y\,3\,x}$ de telle sorte qu'il soit divisible par 495 (base dix).

Déterminer les chiffres x, y, z du nombre $N = \overline{y\,37\,z\,1\,x}$ pour que ce nombre soit divisible par 66 (base dix).

7° On se propose de chercher le reste de la division par 13 du nombre : N = 8 731 579. Montrer qu'on peut utiliser la base douze pour trouver le résultat sans effectuer la division.

2.74 Dans l'ensemble $\mathbb{N}^*$, on considère les deux opérations $\top$ et $\perp$ définies par :

$$a \top b = \Delta(a, b),$$
$$a \perp b = M(a, b).$$

Étudier la commutativité, l'associativité de ces deux lois, la distributivité de chacune d'elles par rapport à l'autre.

Chacune d'elles possède-t-elle un élément neutre?

2.75 On se propose de démontrer que, pour tout groupe fini, le cardinal de tout sous-groupe est un diviseur du cardinal du groupe.

Soit G un groupe, commutatif ou non, e son élément neutre et H un de ses sous-groupes. On notera multiplicativement l'opération interne.

On considère dans G la relation $\mathcal{R}$ définie, quels que soient a et b de G, par

$$\mathcal{R}(a, b) \iff a^{-1}b \in H.$$

a) Démontrer que $\mathcal{R}$ est une relation d'équivalence.

b) Démontrer que la classe de a, modulo $\mathcal{R}$, est l'ensemble des produits ax où x est un élément quelconque de H; on notera cette classe aH.

c) Démontrer que l'application φ_a

$$\varphi_a : H \longrightarrow aH$$
$$x \longmapsto ax$$

est une bijection.

d) On suppose G fini de cardinal n et on pose card $H = p \leqslant n$. Démontrer que p divise n (on remarquera que $\mathcal{R}$ définit une partition de G).

e) On suppose toujours card $G = n$. Démontrer que quel que soit $a \in G$ on a $a^n = e$ (considérer le sous-groupe engendré par a, cf. ex. 2.6).

2.76 On a déjà donné à l'exercice 2.66 une démonstration d'un théorème de FERMAT. En voici deux autres. Dans tout l'exercice p désigne un entier naturel *premier*.

1° Vous avez vu en exercice, en Première, la formule du binôme. Elle est donnée dans ce livre au 3.10 *b*. Elle s'applique à tout anneau commutatif et en particulier à tout corps commutatif.

a) Démontrer que, pour tout entier p premier et tout entier k tel que $1 \leqslant k \leqslant p-1$, C_p^k est divisible par p.

b) Démontrer que, quels que soient $\dot{a}$ et $\dot{b}$ de $\mathbb{Z}/p\,\mathbb{Z}$, on a

$$(\dot{a} + \dot{b})^p = (\dot{a})^p + (\dot{b})^p.$$

En déduire que $(\dot{a} - \dot{b})^p = (\dot{a})^p - (\dot{b})^p$ (Écrire $\dot{a} = (\dot{a} - \dot{b}) + \dot{b}$)). Démontrer par récurrence que, quels que soient $\dot{a}_1 \ldots \dot{a}_n$ de $\mathbb{Z}/p\,\mathbb{Z}$ on a

$$(\dot{a}_1 + \ldots + \dot{a}_n)^p = (\dot{a}_1)^p + \ldots + (\dot{a}_n)^p.$$

c) Déduire de la formule précédente, en faisant $\dot{a}_1 = \ldots = \dot{a}_n = \dot{1}$, que, pour tout n de $\mathbb{N}^*$, on a

$$n^p \equiv n \pmod{p}.$$

2° On pose $G = \mathbb{Z}/p\,\mathbb{Z} - \{\dot{0}\}$ et on considère le groupe $(G, \times)$. Démontrer que, quel que soit l'entier modulo p, $\dot{n} \neq \dot{0}$, on a

$$(\dot{n})^{p-1} = \dot{1}.$$

(Utiliser l'ex. 2.75 e). Conclure.

3| Nombres réels.

Dans la section I *nous faisons précéder l'inventaire des* propriétés fondamentales *de* $\mathbb{R}$ *de considérations destinées à faire bien comprendre le rôle de l'axiome de la borne supérieure.*
La section II *développe ensuite les conséquences des propriétés fondamentales qui font que* $(\mathbb{R}, +, \times, \leqslant)$ *est un* corps commutatif totalement ordonné. *Par une identification consécutive à un certain isomorphisme on montre que* $\mathbb{Q}$ *peut être considéré comme un sous-corps de* $\mathbb{R}$.
Partant de l'ensemble des axiomes de $\mathbb{R}$ *la* section III *presente les* propriétés « topologiques » *de* $\mathbb{R}$: *caractérisation des bornes supérieures et inférieures, parties adjacentes de* $\mathbb{R}$, *propriété des segments emboîtés, propriété d'*ARCHIMÈDE, *densité de* $\mathbb{Q}$ *dans* $\mathbb{R}$; *on démontre en particulier l'existence d'une racine* $n^{\text{ième}}$ *pour tout réel positif et on donne la définition des valeurs approchées à* α^{-n} *près* $(\alpha > 0)$ *d'un nombre réel.*
La section IV *est consacrée à l'étude des* suites infinies *de nombres réels en particulier, conformément au programme, à celle des progressions arithmétiques ou géométriques.*
Le chapitre se termine enfin, c'est la section V, *par l'étude des* calculs approchés *dans* $\mathbb{R}$.

I. Définition axiomatique de $\mathbb{R}$

3. 1 RAPPELS ET COMPLÉMENTS

a) Corps commutatif.

Rappelons (cf. § 2.11 b) que l'on appelle **corps commutatif** tout ensemble K muni de deux lois internes appelées addition et multiplication telles que
i) $(K, +, \times)$ *a une structure d'anneau commutatif* (on désigne par ω *son élément zéro*).
ii) $K^* = K - \{\omega\}$ *est stable pour la multiplication et* $(K^*, \times)$ *est un groupe.*
Nous avons vu aussi que si e est l'élément neutre de la multiplication dans K^*, alors e est l'élément neutre de la multiplication dans K; on l'appelle **élément unité** du corps. Comme $e \in K^*$ on a $e \neq \omega$.
Nous avons vu également qu'un anneau commutatif unitaire d'élément zéro ω et d'élément unité e est un corps si et seulement si $e \neq \omega$ et si tout élément x de K distinct de ω est inversible dans K.
Nous avons vu en Seconde que $(\mathbb{Q}, +, \times)$ et $(\mathbb{R}, +, \times)$ sont des corps commutatifs.

b) Sous-corps d'un corps commutatif.

Définition.

On dit qu'un ensemble H est un **sous-corps** d'un corps commutatif $(K, +, \times)$ si et seulement si

i. H est une partie stable de K pour l'addition et pour la multiplication.

ii. Pour les lois induites sur H par les lois internes de K, $(H, +, \times)$ est un corps commutatif.

Par exemple nous avons vu en Seconde que le corps $\mathbb{Q}$ des nombres rationnels est un sous-corps du corps $\mathbb{R}$ des nombres réels.
Tout corps commutatif est un sous-corps de lui-même. Tout sous-corps de K, distinct de K est appelé **sous-corps propre** de K.

EXERCICE

Démontrer qu'une partie H d'un corps commutatif $(K, +, \times)$ est sous-corps de K si et seulement si

1. H est non vide,
2. $(\forall (x, y) \in H \times H) \quad x - y \in H$.
3. $(\forall (x, y) \in H \times H) \quad xy \in H$.
4. Tout élément x de H, distinct de 0_K, a un inverse dans H.

D'après sa définition, un corps est un cas particulier d'anneau par conséquent toutes les propriétés des anneaux sont applicables aux corps et toutes les notions que l'on peut définir pour les anneaux s'étendent *ipso facto* aux corps. Ainsi si A est un sous-anneau d'un corps K considéré comme anneau nous dirons que A est un **sous-anneau du corps** K. Par exemple l'anneau $\mathbb{Z}$ des entiers relatifs est un sous-anneau du corps $\mathbb{Q}$ des rationnels et du corps $\mathbb{R}$ des réels.

REMARQUE

Inversement étant donné un anneau A il peut arriver qu'un sous-anneau B de A ait une structure de corps. Nous en rencontrerons plusieurs exemples par la suite (cf. § 4.3 ex. 4 et § 4.5 remarque 1).

3. 2 INTRODUCTION A LA DÉFINITION AXIOMATIQUE DE $\mathbb{R}$

a) Le programme ne prévoit pas la construction du corps $\mathbb{Q}$ des rationnels à partir de l'anneau intègre $\mathbb{Z}$; nous la donnons à l'annexe C à la fin de ce volume pour les lecteurs qui seraient intéressés par cette construction.
Le programme prévoit seulement la définition axiomatique de $\mathbb{R}$ — que nous allons donner au § 3.3 — et la mise en évidence de $\mathbb{Q}$ comme sous-corps de $\mathbb{R}$.
Dans ce paragraphe nous supposerons connus $\mathbb{Q}$ et $\mathbb{R}$, que vous avez étudiés en Seconde, de manière à vous faire mieux comprendre l'importance d'un axiome que nous énoncerons dans la définition axiomatique de $\mathbb{R}$ au § 3.3.

b) Vous savez que tout nombre réel positif a une racine carrée dans $\mathbb{R}_+$. En revanche tout nombre rationnel n'a pas forcément une racine carrée dans $\mathbb{Q}_+$.

EXERCICE

Démontrer qu'il n'existe pas de nombre rationnel positif x tel que $x^2 = 2$. (Désignant par $\frac{p}{q}$ le représentant irréductible de x — p et q entiers naturels premiers entre eux — on montrera que $p^2 = 2q^2$ entraîne $p = 2p'$ puis $q = 2q'$.)

L'exercice précédent montre que la racine carrée $\sqrt{2}$ du nombre rationnel 2 appartient à $\mathbb{R}$ mais n'appartient pas à $\mathbb{Q}$.

Étant donnée une partie *majorée* A d'un ensemble ordonné E rappelons que si parmi les majorants de A l'un d'eux est plus petit que tous les autres, *ce plus petit majorant* est appelé **borne supérieure** de A.

De même si A est une partie minorée de E, la **borne inférieure** de A, si elle existe, est *le plus grand des minorants* de A (cf § 1).

Considérons l'ensemble

$$A = \{x \in \mathbb{Q} \mid 0 \leqslant x \quad \text{et} \quad x^2 \leqslant 2\}$$

qui est un sous-ensemble non vide de $\mathbb{Q}$ et de $\mathbb{R}$.

D'après les propriétés que, *dans ce paragraphe*, nous supposons connues, nous avons

$$(\forall x \in A) \qquad 0 \leqslant x \leqslant \sqrt{2}.$$

Cet ensemble A est donc une partie majorée de $\mathbb{Q}$ et, puisque $\mathbb{Q} \subset \mathbb{R}$, de $\mathbb{R}$.

Les majorants de A, *partie de* $\mathbb{R}$, sont tous les **réels** $y \geqslant \sqrt{2}$, l'un d'eux est le plus petit $\sqrt{2}$; la partie A de $\mathbb{R}$ a donc une **borne supérieure dans** $\mathbb{R}$. En revanche les majorants de A, partie de $\mathbb{Q}$ sont tous les **rationnels** $z \geqslant \sqrt{2}$; comme $\sqrt{2} \notin \mathbb{Q}$ les majorants de A dans $\mathbb{Q}$ sont tous les rationnels $z > \sqrt{2}$. Ils constituent l'ensemble

$$M = \{z \in \mathbb{Q} \mid 0 \leqslant z \quad \text{et} \quad 2 < z^2\}.$$

Il est facile de voir que cet ensemble M de rationnels n'a pas de plus petit élément. Supposons qu'il en ait un z_0 montrons que l'on peut trouver un majorant rationnel de M strictement inférieur à z_0. Il suffit de trouver $h \in \mathbb{Q}$ tel que

$$(1) \qquad 0 < h \quad \text{et} \quad 2 < (z_0 - h)^2.$$

La condition $2 < z_0^2 - 2hz_0 + h^2$ est entraînée par $2 < z_0^2 - 2hz_0$

car $$z_0^2 - 2hz_0 \leqslant z_0^2 - 2hz_0 + h^2.$$

Pour que $h \in \mathbb{Q}$ vérifie (1) il suffit donc que l'on ait

$$(2) \qquad 0 < h < \frac{z_0^2 - 2}{2z_0}.$$

Le nombre rationnel z_0 appartenant à M on a $0 \leqslant z_0$ et $2 < z_0^2$; donc $0 < z_0$ et $0 < z_0^2 - 2$; et par conséquent $\frac{z_0^2 - 2}{2z_0}$ est un rationnel strictement positif; on peut donc trouver un rationnel $h > 0$ tel que $(z_0 - h)^2 > 2$: donc z_0 n'est pas le plus petit élément de M. Autrement dit : *la partie* A *de* $\mathbb{Q}$, *partie non vide, majorée de* $\mathbb{Q}$ *n'a pas de borne supérieure dans* $\mathbb{Q}$.

Dans la suite nous oublions ce que nous savons de $\mathbb{Q}$ *et de* $\mathbb{R}$ *et nous allons reprendre l'exposé systématique de leurs propriétés à partir de l'énoncé des propriétés fondamentales de* $\mathbb{R}$ *dont l'ensemble nous donne une définition axiomatique de* $\mathbb{R}$.

3. 3 DÉFINITION AXIOMATIQUE DU CORPS $\mathbb{R}$ DES NOMBRES RÉELS

Conformément au programme nous admettons les résultats suivants :

Il existe un ensemble $\mathbb{R}$, appelé ensemble des **nombres réels** muni d'une addition, d'une multiplication et d'une relation d'ordre notée $\leqslant$ possédant les propriétés suivantes :

I. $(\mathbb{R}, +, \times)$ est un **corps commutatif.** (Nous désignons provisoirement par ω l'élément-zéro et par e l'élément-unité du corps $\mathbb{R}$).

II. $(\mathbb{R}, +, \times, \leqslant)$ est un corps commutatif **totalement ordonné** c'est-à-dire :
La relation notée $\leqslant$ est une relation d'ordre total sur $\mathbb{R}$ et de plus
OA. Quels que soient x, y, z de $\mathbb{R}$ on a

$$(x \leqslant y) \Longrightarrow (x + z \leqslant y + z).$$

OM. Quels que soient x et y de $\mathbb{R}$ on a

$$(\omega \leqslant x \text{ et } \omega \leqslant y) \Longrightarrow (\omega \leqslant xy).$$

III. **B.S.** Toute partie non vide majorée de $\mathbb{R}$ a une borne supérieure dans $\mathbb{R}$.

On résume les propriétés **OA** et **OM** en disant que l'ordre total défini sur $\mathbb{R}$ est compatible avec l'addition et la multiplication dans $\mathbb{R}$.

Nous allons développer les conséquences de ces axiomes en distinguant les propriétés indépendantes de l'axiome **BS** *et celles qui découlent de l'ensemble des propriétés de* $\mathbb{R}$, *donc y compris la propriété* **BS** *(sections II et III).*
Nous étudierons ensuite les suites infinies de nombres réels (section IV) et les calculs approchés dans $\mathbb{R}$ *(section V).*

II. Propriétés de $\mathbb{R}$ considéré comme corps totalement ordonné

3. 4 PROPRIÉTÉS DE $\mathbb{R}$ CONSIDÉRÉ COMME CORPS COMMUTATIF

Rappelons que nous désignons provisoirement par ω l'élément-zéro de $\mathbb{R}$ et par e l'élément-unité de $\mathbb{R}$. On a $\omega \neq e$.

a) Propriétés de $(\mathbb{R}, +)$.

Comme $(\mathbb{R}, +, \times)$ est un corps commutatif, $(\mathbb{R}, +, \times)$ a toutes les propriétés d'un anneau, en particulier

$(\mathbb{R}, +)$ est un groupe commutatif

c'est-à-dire :

$\mathbf{A_1}$. L'addition dans $\mathbb{R}$ est *associative.*
$\mathbf{A_2}$. L'addition dans $\mathbb{R}$ possède un *élément neutre* noté provisoirement ω.
$\mathbf{A_3}$. Tout élément x de $\mathbb{R}$ a un *symétrique* pour l'addition dans $\mathbb{R}$ noté $-x$ et appelé **opposé** de x.
AC. L'addition dans $\mathbb{R}$ est *commutative.*

L'opposé de $-x$ est x, nous dirons que x et $-x$ sont **opposés.**
Ce groupe est appelé **groupe additif** du corps $\mathbb{R}$. Nous avons donc les conséquences suivantes (cf § 2.1 c).

Propriété 1. Quels que soient x, y, z de $\mathbb{R}$ on a

$$(x + z = y + z) \Longrightarrow (x = y),$$

c'est-à-dire tout élément de $\mathbb{R}$ est *régulier* pour l'addition.
Comme pour tout ensemble E muni d'une loi interne notée T, quels que soient x, y, z de E, $x = y$ implique $x \mathbf{T} z = y \mathbf{T} z$ nous pouvons énoncer
Quels que soient x, y, z de $\mathbb{R}$ on a

$$x = y \Longleftrightarrow (x + z = y + z).$$

EXERCICE

1. Montrer que, quels que soient a, b, a', b' de $\mathbb{R}$, on a

$$(a = b \quad \text{et} \quad a' = b') \Longrightarrow (a + a' = b + b').$$

On dit que l'on peut ajouter les égalités membre à membre.
Étendre par récurrence ce résultat à n égalités $a_i = b_i$ $(1 \leqslant i \leqslant n)$.

Propriété 2. *Quels que soient a et b de $\mathbb{R}$ il existe un élément unique de $\mathbb{R}$ tel que*

$$x + a = b.$$

Ce nombre réel noté $b - a$ est appelé *différence* de b et a.

Propriété 3. *Quels que soient x et y de $\mathbb{R}$ on a*

$$-(x + y) = -x - y.$$

EXERCICE

2. Démontrer que quels que soient $a_1, a_2 \ldots, a_n$ de $\mathbb{R}$, on a

$$-(a_1 + a_2 + \ldots + a_n) = -a_1 - a_2 \ldots - a_n.$$

b) Propriétés de $(\mathbb{R}, \times)$.

Les propriétés fondamentales de la multiplication peuvent s'énoncer ainsi en posant $\mathbb{R}^* = \mathbb{R} - \{0\}$.
$\mathbf{M_1}$. La multiplication dans $\mathbb{R}$ est *associative.*
$\mathbf{M_2}$. La multiplication dans $\mathbb{R}$ possède un *élément neutre* noté provisoirement e.
$\mathbf{M_3}$. Tout élément x de $\mathbb{R}^*$ a un *symétrique* pour la multiplication dans $\mathbb{R}$ noté x^{-1} et appelé **inverse** de x.
MC. La multiplication dans $\mathbb{R}$ est *commutative.*
En particulier du fait que $(\mathbb{R}, +, \times)$ soit un corps commutatif (cf. § 2.11 c),

$(\mathbb{R}^*, \times)$ est un groupe commutatif.

Nous dirons que les éléments de $\mathbb{R}^*$ sont les **nombres réels non nuls.**
Ce groupe est appelé **groupe multiplicatif** du corps $\mathbb{R}$.
On voit que l'inverse de x^{-1} est x, nous dirons que x et x^{-1} sont **inverses.**
Nous pourrions énoncer pour $(\mathbb{R}^*, \times)$ trois propriétés analogues aux propriétés 1, 2 et 3 énoncées pour $(\mathbb{R}, +)$; le fait que la multiplication est définie dans $\mathbb{R}$ modifie légèrement les deux premières.

Propriété 1'. Quels que soient x, y, z de $\mathbb{R}$ la relation $x = y$ implique $xz = yz$.

EXERCICE

3. Montrer que, quels que soient a, b, a', b' de $\mathbb{R}$, on a

$$(a = b \quad \text{et} \quad a' = b') \Longrightarrow (aa' = bb').$$

On dit que l'on peut multiplier les égalités membre à membre.
Étendre par récurrence ce résultat à n égalités $a_i = b_i$ $(1 \leqslant i \leqslant n)$.

Supposons que l'on ait $xz = yz$ et $z \neq \omega$; on aura alors

$$(xz)\, z^{-1} = (yz)\, z^{-1};$$

d'où, en utilisant les propriétés de la multiplication,

$$x\,(zz^{-1}) = y\,(zz^{-1}),$$
$$xe = ye,$$
$$x = y.$$

Quels que soient x, y et z de $\mathbb{R}$ on a

$$(xz = yz \quad \text{et} \quad z \neq \omega) \Longrightarrow (x = y)$$

c'est-à-dire : *tout élément* **non nul** de $\mathbb{R}$ est **régulier** pour la multiplication.

Propriété 2'. Soit a un élément quelconque de $\mathbb{R}^*$ et b un élément quelconque de $\mathbb{R}$.
Cherchons x de $\mathbb{R}$ tel que $ax = b$.
Les égalités suivantes sont équivalentes quels que soient a de $\mathbb{R}^*$ et x et b de $\mathbb{R}$:

$$ax = b$$
$$a^{-1}(ax) = a^{-1}b,$$
$$(a^{-1}a)x = a^{-1}b,$$
$$ex = a^{-1}b,$$
$$x = a^{-1}b.$$

Quel que soit a de $\mathbb{R}^*$ et b de $\mathbb{R}$ il existe un nombre réel unique tel que $ax = b$.

Ce nombre réel $x = a^{-1}b = ba^{-1}$ noté aussi $\frac{b}{a}$ est appelé quotient de b par a.

Nous indiquerons au § 3.5 des règles de calcul sur les nombres réels représentés par des quotients de deux nombres réels.

Propriété 3. *Quels que soient x et y de $\mathbb{R}^*$ on a*

$$(xy)^{-1} = x^{-1}y^{-1}.$$

EXERCICE

4. Démontrer que, quels que soient $a_1, a_2, \ldots, a_n$ de $\mathbb{R}^*$ on a

$$(a_1a_2 \ldots a_n)^{-1} = a_1^{-1}a_2^{-1} \ldots a_n^{-1}.$$

c) Propriétés de $(\mathbb{R}, +, \times)$.

En plus des 8 propriétés fondamentales déjà énoncées (A_1, A_2, A_3, AC, M_1, M_2, M_3, MC), $(\mathbb{R}, +, \times)$ ayant toutes les propriétés d'un anneau, nous avons

D. La multiplication dans $\mathbb{R}$ est *distributive* par rapport à l'addition dans $\mathbb{R}$.

On en déduira que l'on a, comme dans tout anneau commutatif (cf § 2.3 c exercices 1 et 2) :

Quels que soient x, y, z de $\mathbb{R}$ on a

$$\omega\, x = x\, \omega = \omega,$$
$$x\,(y - z) = xy - xz,$$
$$(-x)\, y = x\,(-y) = -(xy), \qquad (-x)\,(-y) = xy.$$

Nous savons que tout corps est dépourvu de diviseurs de zéro (cf § 2.11 c); étant donné son importance rappelons cette démonstration (en particulier pour les élèves de la section E).

Supposons que l'on ait $xy = \omega$, ou bien $x = \omega$ et on a $\omega\, y = \omega$ ou bien $x \neq \omega$; dans ce dernier cas on peut appliquer la propriété 2' : la relation $xy = \omega$ est équivalente à $y = \omega\, x^{-1} = \omega$. Concluons

Théorème.

Quels que soient x et y de $\mathbb{R}$ on a

$$(xy = \omega) \iff (x = \omega \quad \text{ou} \quad y = \omega)$$

EXERCICE

5. Démontrer qu'un produit $a_1 a_2 \ldots a_n$ de nombres réels est égal à ω si et seulement s'il existe au moins un facteur $a_i = \omega$.

3. 5 CALCULS SUR LES QUOTIENTS. LINÉARITÉ

a) Calculs sur les quotients.

Quels que soient les réels a et b et les réels *non nuls* a' et b' les égalités suivantes sont équivalentes

$$aa'^{-1} = bb'^{-1},$$
$$a = ba'b'^{-1},$$
$$ab' = ba'.$$

En particulier quel que soit $k \in \mathbb{R}^*$ cette égalité est vérifiée pour $b = ak$ et $b' = a'k$ (régularité de tout $x \neq \omega$ pour la multiplication).

Règle 1. *Quels que soient a, b de $\mathbb{R}$ et a', b' de $\mathbb{R}^*$ on a*

$$\left(\frac{a}{a'} = \frac{b}{b'}\right) \iff (ab' = ba').$$

Pour tout k de $\mathbb{R}^*$ on a

$$\frac{ak}{a'k} = \frac{a}{a'}.$$

D'autre part nous avons (a, b réels quelconques, a', b' réels non nuls quelconques) en appliquant certaines des propriétés énoncées au § 3.4

$$\left(\frac{a}{a'}\right)\left(\frac{b}{b'}\right) = (aa'^{-1})\,(bb'^{-1}) = (ab)\,(a'^{-1}b'^{-1}) = \frac{ab}{a'b'}.$$

Pour la somme nous utilisons de plus la propriété $aa'^{-1} = (ak)\,(a'k)^{-1}$ $(k \neq \omega)$:

$$\left(\frac{a}{a'}\right) + \left(\frac{b}{b'}\right) = aa'^{-1} + bb'^{-1} = (ab')\,(a'b')^{-1} + (ba')\,(a'b')^{-1}$$
$$= (ab' + ba')\,(a'b')^{-1} = \frac{ab' + ba'}{a'b'}.$$

Règle 2. Quels que soient a, b de $\mathbb{R}$ et a', b' de $\mathbb{R}^*$ on a

$$\frac{a}{a'}\,\frac{b}{b'} = \frac{ab}{a'b'}, \quad \frac{a}{a'} + \frac{b}{b'} = \frac{ab' + ba'}{a'b'},$$

EXERCICE

1. Montrer que

$$\left(-\frac{a}{a'}\right) = \frac{-a}{a'} = \frac{a}{-a'} \quad , \quad \frac{a}{a'} - \frac{b}{b'} = \frac{ab' - ba'}{a'b'}.$$

Le quotient $\frac{a}{a'} = aa'^{-1}$ est égal à ω si et seulement si $a = \omega$ puisque a'^{-1}, comme a', est distinct de ω. Supposons $a \neq \omega$ donc $aa'^{-1} \neq \omega$; on a, alors

$$\left(\frac{a}{a'}\right)^{-1} = (aa'^{-1})^{-1} = a^{-1}(a'^{-1})^{-1} = a^{-1}a' = \frac{a'}{a}.$$

Règle 3. *Quels que soient a de $\mathbb{R}$ et a' de $\mathbb{R}^*$ on a*

$$\left(\frac{a}{a'} = \omega\right) \Longleftrightarrow (a = \omega).$$

Si de plus $a \neq \omega$ on a

$$\left(\frac{a}{a'}\right)^{-1} = \frac{a'}{a}.$$

b) Linéarité.

Étant donné un nombre réel quelconque k on appelle **fonction linéaire** de **coefficient** k l'application

$$f_k : \mathbb{R} \longrightarrow \mathbb{R}$$
$$x \longmapsto kx.$$

Cette application vérifie quels que soient les nombres réels x_1, x_2, x, λ,

(1) $$f_k(x_1 + x_2) = k(x_1 + x_2) = kx_1 + kx_2 = f_k(x_1) + f_k(x_2),$$

(2) $$f_k(\lambda x) = k(\lambda x) = \lambda(kx) = \lambda f_k(x).$$

Vous savez que l'on peut considérer $\mathbb{R}$ comme *espace vectoriel sur lui-même*; toute fonction linéaire est donc une *application linéaire* de l'espace vectoriel $\mathbb{R}$ dans lui-même.

Il est évident que f_k est une bijection si et seulement si $k \neq \omega$; dans ce cas la bijection réciproque de f_k est la fonction linéaire $f_{k^{-1}}$.

EXERCICES

2. Démontrer que quels que soient les réels h et k on a

$$f_h \circ f_k = f_k \circ f_h = f_{hk}.$$

En déduire que l'ensemble $\mathfrak{L}(\mathbb{R})$ des fonctions linéaires muni de la composition des applications est un groupe commutatif.

3. Démontrer que toute application f de $\mathbb{R}$ dans $\mathbb{R}$ vérifiant quels que soient λ et x de $\mathbb{R}$

$$f(\lambda x) = \lambda f(x)$$

est une fonction linéaire (faire $x = e$). Quel est son coefficient?

Soit f une fonction linéaire de coefficient k, considérons des nombres réels quelconques $x_1, x_2, \ldots, x_n$, posons

$$y_1 = f(x_1) = kx_1, \ldots, y_i = f(x_i) = kx_i, \ldots, y_n = f(x_n) = kx_n.$$

Si $x_1, x_2, \ldots, x_n$ sont tous non nuls on a

(1) $$\frac{y_1}{x_1} = \ldots = \frac{y_i}{x_i} = \ldots = \frac{y_n}{x_n}.$$

Réciproquement si on a (1) désignons par k la valeur commune des quotients $\frac{y_i}{x_i}$ et par f la fonction linéaire de coefficients k on a pour tout i $(1 \leqslant i \leqslant n)$ on a $y_i = f(x_i)$.

Théorème.

Quelle que soit la suite de nombres réels non nuls $(x_i)_{(1 \leqslant i \leqslant n)}$ et quelle que soit la suite de nombres réels $(y_i)_{1 \leqslant i \leqslant n}$ les propriétés suivantes sont équivalentes

i) $$\frac{y_1}{x_1} = \ldots = \frac{y_i}{x_i} = \ldots = \frac{y_n}{x_n}.$$

ii) Il existe une fonction linéaire f telle que pour tout i $(1 \leqslant i \leqslant n)$ on ait
$$y_i = f(x_i).$$

Nous dirons que *la suite* $(y_i)_{(1 \leqslant i \leqslant n)}$ *est l'image de la suite* $(x_i)_{1 \leqslant i \leqslant n}$ *par la fonction linéaire* f. *Le coefficient* k *de* f *est l'un quelconque des quotients* $\frac{y_i}{x_i}$.

REMARQUE

Un vieil usage consiste à dire que les deux suites (x_i) et (y_i) sont des suites de nombres proportionnels ou encore que l'on a une suite de « rapports » égaux; il est plus simple et plus précis d'utiliser la notion de fonction linéaire.

Conséquence. Si de plus $(\lambda_i)_{(1 \leqslant i \leqslant n)}$ est une suite quelconque de nombres réels tels que
$$\lambda_1 x_1 + \ldots + \lambda_i x_i + \ldots + \lambda_n x_n \neq \omega,$$
on aura
$$\begin{aligned}\lambda_1 y_1 + \ldots + \lambda_i y_i + \ldots + \lambda_n y_n &= \lambda_1 (k x_1) + \ldots + \lambda_i (k x_i) + \ldots + \lambda_n (k x_n) \\ &= k (\lambda_1 x_1 + \ldots + \lambda_i x_i + \ldots + \lambda_n x_n).\end{aligned}$$

Donc dans les conditions données nous avons
$$\left(\frac{y_1}{x_1} = \ldots = \frac{y_n}{x_n}\right) \Longrightarrow \left(\frac{y_1}{x_1} = \ldots = \frac{y_n}{x_n} = \frac{\lambda_1 y_1 + \ldots + \lambda_n y_n}{\lambda_1 x_1 + \ldots + \lambda_n x_n}\right).$$

En particulier si $\frac{y_1}{x_1} = \frac{y_2}{x_2}$ et $x_1 + x_2 \neq \omega$ et $x_1 - x_2 \neq \omega$ on a
$$\frac{y_1}{x_1} = \frac{y_2}{x_2} = \frac{y_1 + y_2}{x_1 + x_2} = \frac{y_1 - y_2}{x_1 - x_2}.$$

EXERCICE

4. Soit deux suites finies *quelconques* de nombres réels (x_i) et (y_i) vérifiant la propriété *ii)* du théorème ci-dessus. On suppose que dans la suite (x_i) il y a au moins un terme non nul.

α) Si $x_k = \omega$ que peut-on dire de y_k?

β) Si $\lambda_1 x_1 + \ldots + \lambda_n x_n = \omega$ que peut-on dire de $\lambda_1 y_1 + \ldots + \lambda_n y_n$?

Toutes les propriétés que nous avons énoncées dans les paragraphes 3.4 *et* 3.5 *utilisent uniquement le fait que* $(\mathbb{R}, +, \times)$ *est un corps commutatif,* **elles sont donc vraies dans tout corps commutatif.**

3. 6 PROPRIÉTÉS DE $\mathbb{R}$ CONSIDÉRÉ COMME CORPS TOTALEMENT ORDONNÉ

a) Relation d'ordre total dans $\mathbb{R}$. Notations et vocabulaire.

La relation notée $\leqslant$ dans $\mathbb{R}$ est une **relation d'ordre total** c'est-à-dire :

O_1. Quel que soit x de $\mathbb{R}$ on a $x \leqslant x$.

O_2. Quels que soient x et y de $\mathbb{R}$ on a

$$(x \leqslant y \quad \text{et} \quad y \leqslant x) \Longrightarrow (x = y).$$

O_3. Quels que soient x, y, z de $\mathbb{R}$ on a

$$(x \leqslant y \quad \text{et} \quad y \leqslant z) \Longrightarrow (x \leqslant z).$$

OT. Quels que soient x, y de $\mathbb{R}$ on a

$$x \leqslant y \quad \text{ou} \quad y \leqslant x.$$

REMARQUE

1. La propriété « O_1 et O_2 » est équivalente à la propriété
   O_1' Quels que soient x et y de $\mathbb{R}$
   $$(x \leqslant y \quad \text{et} \quad y \leqslant x) \Longleftrightarrow (x = y).$$

La *relation réciproque* de la relation notée $\leqslant$ se note $\geqslant$ c'est-à-dire : quels que soient x et y de $\mathbb{R}$ on a

$$(x \geqslant y) \Longleftrightarrow (y \leqslant x)$$

on voit immédiatement que cette relation réciproque de la relation notée $\leqslant$ est aussi une relation d'ordre total.

Quels que soient x et y de $\mathbb{R}$ on pose

$$(x \leqslant y \quad \text{et} \quad x \neq y) \Longleftrightarrow (x < y)$$
$$(x \geqslant y \quad \text{et} \quad x \neq y) \Longleftrightarrow (x > y)$$

$x \leqslant y$ se lit « x **inférieur** à y ».
$x \geqslant y$ — « x **supérieur** à y ».
$x < y$ — « x **strictement inférieur** à y ».
$x > y$ — « x **strictement supérieur** à y ».

REMARQUE

2. Les deux énoncés $(x \leqslant y)$ et $(y \geqslant x)$ sont vrais en même temps, il en est de même de $(x < y)$ et $(y > x)$. Il peut être avantageux de s'imposer la discipline de n'utiliser que les symboles $\leqslant$ et $<$, sans toutefois renoncer à utiliser dans le langage les expressions « supérieur à » et « strictement supérieur à ».

Soient a et b deux nombres réels quelconques tels que $a \leqslant b$, on appelle **intervalle** de $\mathbb{R}$ l'un quelconque des sous-ensembles de $\mathbb{R}$ suivants :

1. $[a, b] = \{x \in \mathbb{R} \mid a \leqslant x \leqslant b\}$ intervalle **fermé** ou **segment**
2. $]a, b[= \{x \in \mathbb{R} \mid a < x < b\}$ intervalle **ouvert**
3. $[a, b[= \{x \in \mathbb{R} \mid a \leqslant x < b\}$ intervalle fermé à gauche, ouvert à droite
4. $]a, b] = \{x \in \mathbb{R} \mid a < x \leqslant b\}$ intervalle ouvert à gauche, fermé à droite

Dans ces quatre cas, bien que dans certains d'entre eux a ou b n'appartiennent pas à l'intervalle, on dit que a et b sont les **extrémités** de l'intervalle considéré. Remarquons que l'on a

$$[a, a] = \{a\} \quad \text{et} \quad]a, a[=]a, a] = [a, a[= \varnothing.$$

Dans les cas suivants les symboles $+\infty$ et $-\infty$ ne représentent pas des nombres réels; ils se lisent respectivement « plus l'infini » et « moins l'infini »; ils ont simplement pour but de permettre l'extension d'une écriture commode.

5. $[a, +\infty[= \{x \in \mathbb{R} \mid a \leqslant x\}$ demi-droite fermée d'origine a.
6. $]a, +\infty[= \{x \in \mathbb{R} \mid a < x\}$ — ouverte d'origine a.
7. $]-\infty, b] = \{x \in \mathbb{R} \mid x \leqslant b\}$ — fermée d'origine b.
8. $]-\infty, b[= \{x \in \mathbb{R} \mid x < b\}$ — ouverte d'origine b.
9. $]-\infty, +\infty[= \mathbb{R}$.

Nous poserons enfin les notations et les définitions suivantes :

$\mathbb{R}_+ = [\omega, +\infty[$ ensemble des nombres réels **positifs**
$\mathbb{R}_+^* =]\omega, +\infty[$ — — **strictement positifs**
$\mathbb{R}_- =]-\infty, \omega]$ — — **négatifs**
$\mathbb{R}_-^* =]-\infty, \omega[$ — — **strictement négatifs**

Les propriétés de la relation d'ordre et ces définitions nous permettent d'écrire

$$\mathbb{R}_+ \cup \mathbb{R}_- = \mathbb{R} \quad , \quad \mathbb{R}_+ \cap \mathbb{R}_- = \{\omega\}.$$

Il en résulte aussi que $\mathbb{R}_+^*$, $\mathbb{R}_-^*$ et $\{\omega\}$ constituent une *partition* de $\mathbb{R}$, il en est de même de $\mathbb{R}_+^*$ et $\mathbb{R}_-$ et de $\mathbb{R}_+$ et $\mathbb{R}_-^*$.

Deux nombres réels, tous deux strictement positifs ou bien tous deux strictement négatifs sont appelés *nombres réels de même signe.*

b) Conséquences de l'axiome OA.

La relation d'ordre total définie sur $\mathbb{R}$ et notée $\leqslant$ est compatible avec l'addition c'est-à-dire

OA. *Quels que soient x, y, z de $\mathbb{R}$ on a*

$$(x \leqslant y) \Longrightarrow (x + z \leqslant y + z)$$

Si on a $x + z \leqslant y + z$ en ajoutant $-z$ aux deux membres on obtient

$$(x + z) + (-z) \leqslant (y + z) + (-z).$$

donc

$$x \leqslant y.$$

Donc, *quels que soient x, y, z de $\mathbb{R}$, on a*

$$(x \leqslant y) \Longleftrightarrow (x + z \leqslant y + z),$$

EXERCICE

1. Démontrer que, quels que soient x, y, z de $\mathbb{R}$, on a
$$(x < y) \Longleftrightarrow (x + z < y + z).$$
2. Démontrer que, quels que soient a, b, a', b' de $\mathbb{R}$, on a
$$(a \leqslant b \quad \text{et} \quad a' \leqslant b') \Longrightarrow (a + a' \leqslant b + b'),$$
$$(a < b \quad \text{et} \quad a' < b') \Longrightarrow (a + a' < b + b').$$

Étendre ces résultats à n inégalités larges (resp. strictes) de même sens.

Quels que soient x et y de $\mathbb{R}$ on a par conséquent

$$(x \leqslant y) \Longleftrightarrow (x - x \leqslant y - x)$$

ce qui est équivalent à $\omega \leqslant y - x$ ou encore $y - x \in \mathbb{R}_+$. Concluons

Théorème.

Quels que soient x et y de $\mathbb{R}$ on a

$$(x \leqslant y) \Longleftrightarrow (y - x \in \mathbb{R}_+),$$
$$(x < y) \Longleftrightarrow (y - x \in \mathbb{R}_+^*),$$

Corollaire.

Quel que soit x de $\mathbb{R}$ on a

$$(x \in \mathbb{R}_+) \Longleftrightarrow (-x \in \mathbb{R}_-),$$
$$(x \in \mathbb{R}_+^*) \Longleftrightarrow (-x \in \mathbb{R}_-^*).$$

c) Conséquences de l'axiome OM.

Rappelons cet axiome

OM. *Quels que soient x et y de* $\mathbb{R}$

$$(\omega \leqslant x \quad \text{et} \quad \omega \leqslant y) \Longrightarrow (\omega \leqslant xy).$$

En utilisant en outre les propriétés du sous-paragraphe précédent, quels que soient x et y de $\mathbb{R}$, on a

$$(\omega \leqslant x \quad \text{et} \quad y \leqslant \omega) \Longrightarrow (xy \leqslant \omega),$$
$$(x \leqslant \omega \quad \text{et} \quad y \leqslant \omega) \Longrightarrow (\omega \leqslant xy).$$

(On appliquera l'axiome **OM** en remplaçant, par exemple, $y \leqslant \omega$ par $\omega \leqslant -y$).
Par récurrence on verra qu'un produit de n nombres réels est *positif* si et seulement s'il contient un *nombre pair* de *facteurs négatifs*.
La relation $xz \leqslant yz$ étant équivalente à $yz - xz \in \mathbb{R}_+$ on voit que l'on a les résultats suivants :

Quels que soient x et y de $\mathbb{R}$ on a

si $\omega \leqslant z$ $\quad [(x \leqslant y) \Longrightarrow (xz \leqslant yz)]$,
si $z \leqslant \omega$ $\quad [(x \leqslant y) \Longrightarrow (yz \leqslant xz)]$.

EXERCICES

3. Quels que soient x et y de $\mathbb{R}$ on a
   si $\omega < z$ $\quad [(x < y) \Longleftrightarrow (xz < yz)]$,
   si $z < \omega$ $\quad [(x < y) \Longleftrightarrow (yz < xz)]$.

4. Démontrer que quels que soient a, a', b, b' *positifs* on a
   $$(a \leqslant b \quad \text{et} \quad a' \leqslant b') \Longrightarrow (aa' \leqslant bb'),$$
   et que quels que soient a, a', b, b' *strictement positifs* on a
   $$(a < b \quad \text{et} \quad a' < b') \Longrightarrow (aa' < bb').$$
   Étendre ce résultat à n inégalités larges (entre nombres *positifs*) et à n inégalités strictes entre nombres *strictement positifs*) de même sens.

Comme vous le savez on pose $xx = x^2$. Si x est positif x^2 est positif; si x est positif, $-x$ est négatif donc $x^2 = (-x)(-x)$ est positif. Le nombre x^2 étant nul si et seulement si x est nul nous pouvons énoncer

Théorème.

Le carré de tout nombre réel est positif. Le carré de tout nombre réel non nul est strictement positif.

L'élément unité $e = e^2$ est donc positif, comme $e \neq \omega$ nous pouvons dire

Corollaire.

Dans $\mathbb{R}$ on a

$$\omega < e.$$

EXERCICE

5. Démontrer que si $x \neq \omega$, alors x et x^{-1} sont de même signe.

3. 7 $\mathbb{Z}$ CONSIDÉRÉ COMME SOUS-ANNEAU DU CORPS $\mathbb{R}$. CORPS $\mathbb{Q}$ DES NOMBRES RATIONNELS

a) Anneau $e\mathbb{Z}$.

Soit n un entier relatif quelconque, nous désignerons par ne le nombre réel défini de la manière suivante

si $0 < n$ $\quad ne = e + e + \ldots + e$ (n termes)
si $0 = n$ $\quad ne = \omega$
si $n < 0$ $\quad ne = (-n)(-e) = -e - e \ldots - e$ ($-n$ termes)

On voit que pour tout n de $\mathbb{Z}$ on a

$$-(ne) = (-n)\,e.$$

On remarquera que, *pour l'instant*, on ne sait pas si $n \in \mathbb{R}$, alors que $ne \in \mathbb{R}$.
Nous noterons $e\mathbb{Z}$ l'ensemble de tous les nombres réels de la forme ne, n étant un entier relatif quelconque.
Vous démontrerez facilement que, quels que soient n et p de $\mathbb{Z}$, on a

(1) $\quad ne + pe = (n + p)\,e,$
(2) $\quad (ne)(pe) = (np)\,e.$

Ces deux égalités sont vérifiées de façon évidente si $n = 0$ ou $p = 0$. On peut donc supposer $n \neq 0$ et $p \neq 0$.
Pour (1), la vérification est immédiate pour $0 < n$ et $0 < p$, de même pour $n < 0$ et $p < 0$. Pour $0 < n$ et $p < 0$ il faudra considérer trois cas $|p| < n$, $|p| = n$, $n < |p|$.
Pour (2) il faudra considérer aussi trois cas $0 < n$, $0 < p$ puis $n < 0$, $p < 0$ et enfin $0 < n$ et $p < 0$; par exemple dans ce dernier cas on aura :

$$(ne)(pe) = (ne)\,[(-p)(-e)] = \underbrace{(e + \ldots + e)}_{n \text{ termes}}\ \underbrace{[(-e) + \ldots + (-e)]}_{-p \text{ termes}}$$

$$= \underbrace{(-e^2) + (-e^2) + \ldots + (-e^2)}_{n(-p) \text{ termes}}$$

$$= [n(-p)]\,(-e) = (-np)(-e) = (np)\,e.$$

D'autre part le fait que $\omega < e$ et l'axiome **OA** impliquent que $\omega + \omega < e + e$ c'est-à-dire $\omega < 2e$; on voit facilement, par récurrence, que, pour tout n de $\mathbb{N}^*$, on a $\omega < ne$; comme $(-n)\,e = -(ne)$ on a, pour tout n de $\mathbb{N}^*$, $(-n)\,e < \omega$.

Récapitulons les propriétés du symbole ne.

Lemme.

Quels que soient les entiers relatifs n et p on a

(1) $ne + pe = (n + p)\, e$,

(2) $(ne)\,(pe) = (np)\, e$,

(3) si $0 < n$ $\quad \omega < ne$,
si $0 = n$ $\quad \omega = ne$,
si $n < 0$ $\quad ne < \omega$.

Ces propriétés peuvent s'interpréter très facilement en introduisant l'application

$$f : \mathbb{Z} \longrightarrow e\mathbb{Z}$$
$$n \longmapsto ne.$$

L'ensemble $e\mathbb{Z}$ étant l'ensemble de *tous* les nombres réels de la forme ne ($n \in \mathbb{Z}$) l'application f est *surjective*.

Les propriétés (1) et (2) du lemme montrent d'une part que $e\mathbb{Z}$ est une *partie stable* de $\mathbb{R}$ pour l'addition et la multiplication des réels, donc ces opérations sont des *lois internes* définies sur $e\mathbb{Z}$. D'autre part les égalités (1) et (2) peuvent s'écrire

(4) $\qquad f(n + p) = f(n) + f(p)$

(5) $\qquad f(np) \quad = f(n)\, f(p)$

et ceci quels que soient les entiers relatifs n et p donc f définit un *homomorphisme* de $(\mathbb{Z}, +, \times)$ dans $(e\mathbb{Z}, +, \times)$.

Nous avons vu que f est *surjective*, montrons que f est *injective*. Quel que soit p de $\mathbb{Z}$, on a $f(-p) = -f(p)$. Il en résulte que quels que soient n et p de $\mathbb{Z}$ la relation

$$f(n) = f(p) \quad \text{ou} \quad f(n) - f(p) = \omega$$

peut s'écrire $\qquad f(n) + f(-p) = \omega$,

c'est-à-dire $f\ [n + (-p)] = f(n - p) = \omega$ ou encore $(n - p)\, e = \omega$;

la propriété 3 du lemme montre que l'on a $n - p = \omega$ c'est-à-dire $n = p$; l'application f est donc *injective*.

L'homomorphisme f est donc bijectif; c'est un *isomorphisme* de $(\mathbb{Z}, +, \times)$ sur $(e\mathbb{Z}, +, \times)$; l'addition et la multiplication dans $e\mathbb{Z}$ ont donc exactement les mêmes propriétés que l'addition et la multiplication dans $\mathbb{Z}$; or $(\mathbb{Z}, +, \times)$ est un anneau commutatif il en résulte que $(e\mathbb{Z}, +, \times)$ est aussi un *anneau commutatif*, il est isomorphe à l'anneau $\mathbb{Z}$.

D'autre part soit deux entiers relatifs n et p vérifiant $n < p$ on aura

$$f(n) - f(p) = f(n - p) < \omega \quad \text{donc} \quad f(n) < f(p)$$

puisque $n - p < 0$ (propriété 3 du lemme).

Donc f est une application strictement croissante de $\mathbb{Z}$ sur $e\mathbb{Z}$. Concluons

Théorème.

Quels que soient les entiers relatifs n, p la bijection $f : n \longmapsto ne$ de $\mathbb{Z}$ sur $e\mathbb{Z}$ est telle que

(4) $\qquad f(n + p) = f(n) + f(p)$,

(5) $\qquad f(np) \quad = f(n)\, f(p)$,

(6) $\qquad (n < p) \Longrightarrow (f(n) < f(p))$.

Nous traduirons ces propriétés en disant que $f : n \longmapsto ne$ de $\mathbb{Z}$ sur $e\mathbb{Z}$ est un **isomorphisme** de $(\mathbb{Z}, +, \times, \leqslant)$ sur $(e\mathbb{Z}, +, \times, \leqslant)$ à la fois pour l'addition, la multiplication et l'ordre total définis respectivement sur $\mathbb{Z}$ et $e\mathbb{Z}$.
Or $(\mathbb{Z}, +, \times, \leqslant)$ est un anneau commutatif totalement ordonné, grâce au fait que f est une bijection et aux propriétés (4), (5), (6) on voit immédiatement que $(e\mathbb{Z}, +, \times, \leqslant)$ est un **anneau commutatif totalement ordonné.**

Les propriétés de l'addition, de la multiplication et de l'ordre défini respectivement sur $\mathbb{Z}$ et $e\mathbb{Z}$ étant les mêmes il n'y a aucun inconvénient à **identifier l'élément** n **de** $\mathbb{Z}$ **avec l'élément** ne **de** $\mathbb{R}$. En particulier

$$0 = \omega \quad , \quad 1 = e,$$

et, moyennant cette identification, on a

$$\mathbb{Z} \subset \mathbb{R};$$

de plus $\mathbb{Z}$ identifié à $e\mathbb{Z}$ est une partie stable de $\mathbb{R}$ pour l'addition et la multiplication et $(\mathbb{Z}, +, \times)$ ayant une structure d'anneau, l'anneau $\mathbb{Z}$ peut être considéré comme un **sous-anneau** du corps $\mathbb{R}$ (cf § 3.1 b).
D'autre part la propriété (6) montre que l'ordre défini sur $\mathbb{R}$ se réduit bien pour la partie $\mathbb{Z}$ de $\mathbb{R}$ à l'ordre déjà défini sur $\mathbb{Z}$; on a, en particulier

$$\mathbb{N} = \mathbb{Z}_+ \subset \mathbb{R}_+.$$

Désormais nous noterons les éléments zéro et unité de $\mathbb{R}$ exclusivement par les symboles 0 et 1.

b) Corps $\mathbb{Q}$ des nombres rationnels.

Le fait que $\mathbb{Z} \subset \mathbb{R}$ nous permet de dire que le quotient de $a \in \mathbb{Z}$ par $b \in \mathbb{Z}^*$ est un nombre réel (cf § 3.4 b, propriété 2'); nous poserons la définition suivante :

Définition.

On appelle **nombre rationnel** tout nombre réel égal au quotient d'un entier relatif par un entier relatif non nul.
L'ensemble des nombres rationnels est noté $\mathbb{Q}$.

Tout entier relatif n étant le quotient de n par 1 est un nombre rationnel; comme tout rationnel est un réel nous avons

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Un entier tel que 2 n'a pas d'inverse dans $\mathbb{Z}$, il en a un dans $\mathbb{Q}$ le nombre rationnel $\frac{1}{2}$; donc $\frac{1}{2} \in \mathbb{Q}$ et $\frac{1}{2} \notin \mathbb{Z}$ donc $\mathbb{Z} \neq \mathbb{Q}$. Nous verrons au § 3.11 a que $\mathbb{Q} \neq \mathbb{R}$ (il nous faudra pour démontrer cela utiliser l'axiome **BS**).
Ainsi à tout couple (a, a') de $\mathbb{Z} \times \mathbb{Z}^*$ est associé un nombre rationnel unique x, quotient de a par a'. Un tel couple (a, a') est appelé **fraction** de *numérateur* a et de *dénominateur* a'. Réciproquement des fractions distinctes (a, a'), (b, b') définissent un même rationnel x si et seulement si $ab' = ba'$ (cf. § 3.5 a règle 1). Il est évident que la relation dans $\mathbb{Z} \times \mathbb{Z}^*$ « (a, a') et (b, b') définissent un même rationnel » est une *relation d'équivalence*; un nombre rationnel est donc associé à une et une seule classe d'équivalence de fractions pour cette relation. Si $x = \frac{a}{a'}$, nous dirons que la fraction (a, a') est un représentant du nombre rationnel $x = \frac{a}{a'}$.

REMARQUE

Traditionnellement une fraction s'écrit $\frac{a}{a'}$ et non (a, a'). Il y a là un abus de langage consistant à confondre classe et représentant. Lorsque nous voudrons considérer $\frac{a}{a'}$ comme fraction nous dirons « soit la fraction $\frac{a}{a'}$ ». Ainsi les deux *fractions* $\frac{2}{3}$ et $\frac{10}{15}$ sont des *fractions équivalentes* mais pas des fractions égales; d'ailleurs en tant que fractions elles n'ont pas les mêmes propriétés, seule la fraction $\frac{2}{3}$ est irréductible, c'est-à-dire 2 et 3 sont premiers entre eux; en revanche les *nombres rationnels* $\frac{2}{3}$ et $\frac{10}{15}$ sont *égaux*.

EXERCICE

Montrer que tout nombre rationnel x admet un représentant unique $\frac{a}{a'}$ tel que la fraction $\frac{a}{a'}$ soit *irréductible* et a' *strictement positif*; on l'appelle le représentant *canonique* de x.

Soit x et y deux nombres rationnels quelconques de représentants respectifs quelconques $\frac{a}{a'}$ et $\frac{b}{b'}$; les règles de calculs sur les quotients (cf. § 3.5 a) montrent que

$$x - y = \frac{a}{a'} - \frac{b}{b'} = \frac{ab' - ba'}{a'b'} \in \mathbb{Q}.$$

Or $\mathbb{Q}$ est une partie non vide de $\mathbb{R}$, puisque $\mathbb{Z} \subset \mathbb{Q}$, donc (cf. § 2.6 a) $(\mathbb{Q}, +)$ est un *sous-groupe* de $(\mathbb{R}, +)$.

D'autre part

$$xy = \frac{a}{a'} \times \frac{b}{b'} = \frac{ab}{a'b'} \in \mathbb{Q};$$

donc $\mathbb{Q}$ est une *partie stable* de $\mathbb{R}$ pour la multiplication des nombres réels.

Enfin quel que soit le représentant $\frac{a}{a'}$ du rationnel x on a

$$(x \neq 0) \iff (a \neq 0)$$

et dans ce cas (cf. § 3.5 a)

$$x^{-1} = \frac{a'}{a} \in \mathbb{Q}.$$

Concluons (cf. exercice du § 3.1 b).

Théorème.

L'ensemble $\mathbb{Q}$ des nombres rationnels muni de l'addition et de la multiplication des nombres réels est un **sous-corps** du corps commutatif $\mathbb{R}$.

c) Corps totalement ordonné $(\mathbb{Q}, +, \times, \leqslant)$.

L'ordre total défini sur $\mathbb{R}$ détermine un ordre total sur $\mathbb{Q}$ que nous noterons également $\leqslant$. Nous poserons

$$\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid 0 \leqslant x\},$$
$$\mathbb{Q}_- = \{x \in \mathbb{Q} \mid x \leqslant 0\},$$
$$\mathbb{Q}_+^* = \{x \in \mathbb{Q} \mid 0 < x\},$$
$$\mathbb{Q}_-^* = \{x \in \mathbb{Q} \mid x < 0\}.$$

Cet ordre est, dans $\mathbb{R}$, *compatible* avec l'*addition* et la *multiplication*.
Donc $(\mathbb{Q}, +, \times, \leqslant)$ est un **corps commutatif totalement ordonné.**
La relation $x \leqslant y$ dans $\mathbb{Q}$ peut s'écrire $y - x \in \mathbb{R}_+$ avec $y - x \in \mathbb{Q}$; elle s'écrit donc $y - x \in \mathbb{Q}_+$.

Nous reprenons maintenant l'exposé des propriétés de $\mathbb{R}$. *Rappelons que, comme* $\mathbb{Z} \subset \mathbb{R}$, *nous notons désormais 0 et 1 l'élément zéro et l'élément unité de* $\mathbb{R}$.

3. 8 VALEUR ABSOLUE ET DISTANCE

a) Valeur absolue d'un nombre réel.

Définition.
On appelle **valeur absolue** du nombre réel x le nombre réel noté $|x|$ défini par
$$|x| = \sup(x, -x).$$

Le nombre réel $|x|$ est donc **positif,** c'est le plus grand des deux nombres x et $-x$ donc

$$|x| = \begin{cases} x & \text{si} \quad 0 \leqslant x, \\ -x & \text{si} \quad x \leqslant 0. \end{cases}$$

Il résulte également de la définition que, quel que soit x, on a

$$|-x| = |x|$$

et quels que soient x et y de $\mathbb{R}$ on a

$$(|x| = |y|) \iff (x = y \quad \text{ou} \quad x = -y)$$

Enfin quel que soit x de $\mathbb{R}$ on a

$$-|x| \leqslant x \leqslant |x|;$$

il en résulte que quels que soient $x \in \mathbb{R}$ et $a \in \mathbb{R}_+$ on a

$$(|x| \leqslant a) \iff (-a \leqslant x \leqslant a).$$

Propriétés fondamentales de la valeur absolue d'un nombre réel.

Si $x = 0$ alors $|x| = 0$. Si $x \neq 0$ on a $x < 0$ ou bien $0 < x$, donc $|x| \neq 0$. Concluons

$$(\forall x \in \mathbb{R}) \quad (x = 0) \iff (|x| = 0).$$

Cherchons la valeur absolue du produit xy de deux réels quelconques. Le nombre $|xy|$ est le plus grand des deux nombres xy et $-(xy)$; or

$$-(xy) = (-x)\,y = x\,(-y)$$

et

$$xy = (-x)\,(-y).$$

Donc $|xy|$ *est égal à ceux des produits* xy, $(-x)\,y$, $x\,(-y)$, $(-x)\,(-y)$ *qui sont positifs.* Or $|x|$ (resp. $|y|$) est égal à celui des nombres x et $-x$ (resp. y et $-y$) qui est positif. *Donc* $|x|\,|y|$ *est égal à ceux des produits* xy, $(-x)\,y$, $x\,(-y)$, $(-x)\,(-y)$ *qui sont positifs.* On a donc

$$|xy| = |x|\,|y|$$

Considérons la somme $x + y$ de deux réels quelconques; on a

$$-|x| \leqslant x \leqslant |x|,$$
$$-|y| \leqslant y \leqslant |y|;$$

d'où en appliquant la compatibilité de l'ordre et de l'addition dans $\mathbb{R}$ on obtient

$$-(|x| + |y|) \leqslant x + y \leqslant |x| + |y|,$$

relation qui, comme nous venons de le voir ci-dessus est équivalente à

$$|x + y| \leqslant |x| + |y|.$$

Théorème.

Quels que soient x et y de $\mathbb{R}$ on a

V_1	$(|x| = 0) \iff (x = 0)$,
V_2	$|xy| = |x|\ |y|$,
V_3	$|x + y| \leqslant |x| + |y|$.

REMARQUE

D'une manière générale étant donné un corps commutatif K, d'élément zéro ω, on appelle **valeur absolue** sur K toute application de K dans $\mathbb{R}_+$.

$$v : K \longrightarrow \mathbb{R}_+$$

telle que quels que soient x et y de K on a

V_1	$(v(x) = 0) \iff (x = \omega)$
V_2	$v(xy) = v(x)\, v(y)$
V_3	$v(x + y) \leqslant v(x) + v(y)$.

Par abus de langage on dit aussi que $v(x)$ est une valeur absolue de x — c'est ce que nous avons fait pour $\mathbb{R}$.

Tout corps K pour lequel on peut définir une valeur absolue est appelé **corps valué**. *Ainsi* $\mathbb{R}$ *et* $\mathbb{Q}$ *sont des corps valués.*

Des propriétés fondamentales de la valeur absolue on peut en déduire d'autres.

Si $x \neq 0$ la relation $xx^{-1} = 1$ nous donne $|x|\,|x^{-1}| = 1$ c'est-à-dire

$$(\forall x \in \mathbb{R}^*) \quad \left|\frac{1}{x}\right| = \frac{1}{|x|}.$$

Donc quels que soient $x \in \mathbb{R}$ et y de $\mathbb{R}^*$, $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$.

D'autre part, comme $|y| = |-y|$, on a

$$|x - y| = |x + (-y)| \leqslant |x| + |-y| = |x| + |y|$$

Appliquons cette relation à $y = (x + y) - x$ on a

$$|y| \leqslant |x + y| + |x|$$

c'est-à-dire

$$|y| - |x| \leqslant |x + y|.$$

En transposant x et y on obtient

$$|x| - |y| \leqslant |x + y|.$$

Or les deux nombres $|y| - |x|$ et $|x| - |y|$ sont opposés; on a donc $\big||x| - |y|\big| \leqslant |x + y|$ et par conséquent quels que soient x et y de $\mathbb{R}$

$$\big||x| - |y|\big| \leqslant |x + y| \leqslant |x| + |y|.$$

Enfin vous montrerez facilement par récurrence que l'on a, quels que soient $x_1, \ldots, x_n$.

$$|x_1 x_2 \ldots x_n| = |x_1|\,|x_2| \ldots |x_n|,$$
$$|x_1 + x_2 + \ldots + x_n| \leqslant |x_1| + |x_2| + \ldots + |x_n|.$$

Nous écrirons ces relations sous la forme plus condensée

$$\left|\prod_{i=1}^{i=n} x_i\right| = \prod_{i=1}^{i=n} |x_i|,$$
$$\left|\sum_{i=1}^{i=n} x_i\right| \leqslant \sum_{i=1}^{i=n} |x_i|.$$

EXERCICES

1. On considère l'application $x \longmapsto |x|$ de $\mathbb{R}$ dans $\mathbb{R}_+$; est-elle surjective? injective?
   Définit-elle un homomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+, +)$? de $(\mathbb{R}, \times)$ dans $(\mathbb{R}_+, \times)$?
2. Dans quel cas a-t-on $|x + y| = |x| + |y|$? $|x + y| = \big||x| - |y|\big|$?

b) Distance définie sur $\mathbb{R}$.

Définition.

On appelle **distance** définie sur un ensemble E toute application

$$d : E \times E \longrightarrow \mathbb{R}_+$$
$$(x, y) \longmapsto d(x, y)$$

qui possède les propriétés suivantes :

D_1. Quels que soient x *et* y de E

$$(d(x, y) = 0) \Longleftrightarrow (x = y).$$

D_2. Quels que soient x et y de E

$$d(y, x) = d(x, y).$$

D_3. Quels que soient x, y, z de E on a

$$d(x, y) \leqslant d(x, z) + d(z, y).$$

Tout ensemble E muni d'une distance d, soit (E, d) est appelé **espace métrique.**

Par abus de langage le nombre $d(x, y)$ est appelé distance de x et y, pour la distance d. Considérons l'application d suivante :

$$d : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}_+$$
$$(x, y) \longmapsto |x - y|.$$

On voit immédiatement que les propriétés $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{D_3}$ sont vérifiées; en effet quels que soient x, y, z de $\mathbb{R}$ on a

$$(d(x, y) = 0) \Longleftrightarrow (|x - y| = 0) \Longleftrightarrow (x - y),$$
$$d(y, x) = |y - x| = |x - y| = d(x, y),$$
$$d(x, y) = |x - y| = |(x - z) - (y - z)| \leqslant |x - z| + |y - z|$$
$$= d(x, z) + d(z, y).$$

L'application d est donc une distance définie sur $\mathbb{R}$. On voit immédiatement que les restrictions de d à $\mathbb{Q} \times \mathbb{Q}$ et à $\mathbb{Z} \times \mathbb{Z}$ vérifient toujours les propriétés $\mathbf{D_1}$, $\mathbf{D_2}$, $\mathbf{D_3}$ donc

Munis de la distance $(x, y) \longmapsto |x - y|$ *les ensembles* $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ *sont des* **espaces métriques.**

3. 9 PUISSANCES ENTIÈRES D'UN NOMBRE RÉEL

a) Puissances entières (exposant strictement positif) d'un nombre réel quelconque.

Pour tout nombre réel a et tout entier $n \geqslant 1$ on pose

$$a^1 = a \quad \text{et} \quad a^{n+1} = a^n\, a.$$

Le symbole a^n se lit « a **exposant** n » ou « a **puissance** n »; cependant a^2 se lit « *a au carré* » et a^3 « *a au cube* ».

Pour tout $n \geqslant 1$ on a

$$0^n = 0 \quad \text{et} \quad 1^n = 1.$$

Prenons $n \geqslant 1$ quelconque par définition on a $a^n\, a^1 = a^n\, a = a^{n+1}$; supposons vraie la formule $a^n\, a^p = a^{n+p}$ (hypothèse de récurrence sur $p \geqslant 1$); nous avons

$$a^n\, a^{p+1} = a^n\, (a^p . a) = (a^n\, a^p)\, a = a^{n+p}\, a = a^{n+p+1};$$

la formule $a^n\, a^p = a^{n+p}$ est donc démontrée quels que soient les entiers $n \geqslant 1$ et $p \geqslant 1$.
De même on a $(ab)^1 = ab = a^1\, b^1$; supposons $(ab)^n = a^n\, b^n$ (hypothèse de récurrence sur n); nous avons

$$(ab)^{n+1} = (ab)^n\, (ab) = (a^n\, b^n)\, (ab) = (a^n\, a)\, (b^n\, b) = a^{n+1}\, b^{n+1};$$

la formule $(ab)^n = a^n\, b^n$ est donc démontrée quel que soit l'entier $n \geqslant 1$.
Prenons enfin un entier $n \geqslant 1$ quelconque; par définition on a $(a^n)^1 = a^n = a^{n \times 1}$; supposons vraie la formule $(a^n)^p = a^{np}$ (hypothèse de récurrence sur $p \geqslant 1$); nous avons

$$(a^n)^{p+1} = (a^n)^p\, a^n = a^{np}\, a^n = a^{np+n} = a^{n\,(p+1)};$$

la formule $(a^n)^p = a^{np}$ est donc démontrée quels que soient les entiers $n \geqslant 1$ $p \geqslant 1$.
Quels que soient les nombres réels a et b et quels que soient les entiers $n \geqslant 1$ et $p \geqslant 1$ on a

(1) $$a^n\, a^p = a^{n+p}$$

(2) $$(ab)^n = a^n\, b^n,$$

(3) $$(a^n)^p = a^{np}.$$

EXERCICE 1

1. Démontrer que, quels que soient $a \in \mathbb{R}^*$ et les entiers $n \geqslant 1$ et $p \geqslant 1$ on a

$$\frac{a^n}{a^p} = \begin{cases} a^{n-p} & \text{si } p < n \\ 1 & \text{si } p = n \\ \dfrac{1}{a^{p-n}} & \text{si } n < p \end{cases}$$

REMARQUE

1. Dans tout corps et même dans tout anneau A on pose, quel que soit $a \in A$ et quel que soit l'entier $n \geqslant 1$

$$a^1 = a \qquad a^{n+1} = a^n a.$$

Les formules (1) et (3) sont valables dans tout anneau, la formule (2) est vraie dans tout anneau commutatif.

b) Puissances entières d'un nombre réel non nul.

La formule (1) ci-dessus montre que l'application

$$g_1 : \mathbb{N}^* \longrightarrow \mathbb{R}, \quad n \longmapsto a^n$$

est un *homomorphisme* de $(\mathbb{N}^*, +)$ dans $(\mathbb{R}, \times)$; en effet la formule (1) s'écrit quels que soient n et p de $\mathbb{N}^*$

$$g_1(n+p) = g_1(n)\, g_1(p).$$

Cherchons un *prolongement* g de g_1 à $\mathbb{Z}$ tout entier qui soit encore un *homomorphisme* de $(\mathbb{Z}, +)$ dans $(\mathbb{R}, \times)$. Si g existe nous aurons quels que soient n et p de $\mathbb{Z}$

$$g(n+p) = g(n)\, g(p).$$

Faisons apparaître des **conditions nécessaires.** Pour tout n de $\mathbb{N}^*$ on a

$$g(n) = g_1(n) = a^n.$$

Pour tout n de $\mathbb{N}^*$ et $p = 0$ on aura

$$g(n+0) = g(n) = g(n)\, g(0).$$

Or $g(n) = a^n$ est **non nul** si et seulement si $a \neq 0$.
Supposons a **non nul** on aura

$$g(0) = 1.$$

Dans les mêmes conditions ($a \neq 0$) quels que soient l'entier $n \geqslant 1$ nous aurons

$$1 = g(0) = g(n-n) = g(n)\, g(-n);$$

donc pour tout n de $\mathbb{N}^*$ on aura

$$g(-n) = \frac{1}{g(n)}.$$

Nous sommes ainsi amenés à poser quel que soit $a \in \mathbb{R}^*$ et quel que soit n de $\mathbb{N}^*$

$$a^0 = 1 \quad , \quad a^{-n} = \frac{1}{a^n}.$$

Appliqué à $n = 1$ cette définition justifie la notation a^{-1} adoptée pour l'*inverse de tout réel non nul* a.

Reste à prouver que les conditions trouvées sont bien **suffisantes,** c'est-à-dire que g défini comme il a été dit pour $a \in \mathbb{R}^*$ et $n \in \mathbb{Z}$ est bien un homomorphisme de $(\mathbb{Z}, +)$ dans $(\mathbb{R}, \times)$.

La formule

$$a^{n+p} = a^n\, a^p$$

a été démontrée pour $n > 0$ et $p > 0$; supposons $a \neq 0$ en tenant compte de $a^0 = 1$ on voit qu'elle est vraie quels que soient n et p de $\mathbb{N}$. Il suffit donc de la démontrer pour $n \geqslant 0$ et $p \leqslant 0$ et pour $n \leqslant 0$ et $p \leqslant 0$, la commutativité de la multiplication nous dispensant d'étudier le cas $n \leqslant 0$ et $p \geqslant 0$.

Premier cas : $n \geqslant 0$, $p \leqslant 0$; posons $p = -p'$, alors $0 \leqslant p'$ et nous avons

$$a^n a^p = a^n a^{-p'} = \frac{a^n}{a^{p'}};$$

d'où (cf. exercice 1 ci-dessus) :
si $p' \leqslant n$ on a

$$a^n a^p = \frac{a^n}{a^{p'}} = a^{n-p'} = a^{n+p};$$

si $n < p'$ (alors $p' - n > 0$)

$$a^n a^p = \frac{a^n}{a^{p'}} = \frac{1}{a^{p'-n}} = a^{-(p'-n)} = a^{-p'+n} = a^{n+p}.$$

Deuxième cas : $n \leqslant 0$ et $p \leqslant 0$; posons $n = -n'$, $p = -p'$, alors $0 \leqslant n'$ et $0 \leqslant p'$ et on a

$$a^n a^p = a^{-n'} a^{-p'} = \frac{1}{a^{n'}} \frac{1}{a^{p'}} = \frac{1}{a^{n'} a^{p'}} = \frac{1}{a^{n'+p'}} = a^{-(n'+p')}$$
$$= a^{-n'-p'} = a^{n+p}.$$

Conclusion.

Pour tout nombre réel a et tout entier relatif x le symbole a^x a le sens suivant :
Si $x = n > 0$ $\quad a^1 = a$ et $a^{n+1} = a^n a$.
Si $x = 0$ et $a \neq 0$ $\quad a^0 = 1$.
Si $x = -n < 0$ $\quad a^{-n} = \frac{1}{a^n}$.

Nous avons vu, de plus, que pour tout $a \in \mathbb{R}^*$ *l'application*

$$g : \mathbb{Z} \longrightarrow \mathbb{R}$$
$$n \longmapsto a^n$$

est un homomorphisme de $(\mathbb{Z}, +)$ *dans* $(\mathbb{R}, \times)$; c'est-à-dire que, quels que soient a de $\mathbb{R}^*$ et n et p de $\mathbb{Z}$, on a

(1′) $$a^{n+p} = a^n a^p.$$

En particulier on a, pour tout n de $\mathbb{Z}$ $(a \neq 0)$,

$$a^n a^{-n} = 1.$$

Étendons à $\mathbb{Z}$ les formules (2) et (3) du sous-paragraphe précédent.
Soient a et b deux réels non nuls quelconques et un entier $n \leqslant 0$, posons $n' = -n$, alors $n' \geqslant 0$ d'où

$$(ab)^n = (ab)^{-n'} = \frac{1}{(ab)^{n'}} = \frac{1}{a^{n'} b^{n'}} = a^{-n'} b^{-n'} = a^n b^n.$$

En particulier la relation $aa^{-1} = 1$ nous donne, quel que soit n de $\mathbb{Z}$, $a^n (a^{-1})^n = 1$ d'où

(4) $$(a^{-1})^n = (a^n)^{-1} = a^{-n}.$$

Soit à démontrer la formule $(a^n)^p = a^{np}$ quels que soient a de $\mathbb{R}^*$ et n et p de $\mathbb{Z}$. Elle a déjà été démontrée pour $n > 0$ et $p > 0$; comme $a^0 = 1$ elle est vraie quels que soient n et p de $\mathbb{N}$. Il nous reste ici trois cas à étudier, car n et p jouent des rôles différents.

Premier cas: $n \geqslant 0$ et $p \leqslant 0$; posons $p' = -p$, alors $p' \geqslant 0$; d'où

$$(a^n)^p = (a^n)^{-p'} = \frac{1}{(a^n)^{p'}} = \frac{1}{a^{np'}} = \frac{1}{a^{-(np)}} = a^{np}.$$

Deuxième cas : $n \leqslant 0$ et $p \geqslant 0$; posons $n' = -n$, alors $n' \geqslant 0$; d'où

$$(a^n)^p = (a^{-n'})^p = \left(\frac{1}{a^{n'}}\right)^p = \frac{1}{a^{n'p}} = \frac{1}{a^{-(np)}} = a^{np}$$

car

$$\left(a^{n'}\,\frac{1}{a^{n'}}\right)^p = (a^{n'})^p \left(\frac{1}{a^{n'}}\right)^p = a^{n'p}\left(\frac{1}{a^{n'}}\right)^p = 1$$

donc $a^{n'p}$ et $\left(\frac{1}{a^{n'}}\right)^p$ sont inverses.

Troisième cas : $n \leqslant 0$ et $p \leqslant 0$; posons $n' = -n$ et $p' = -p$ on a $0 \leqslant n'$ et $0 \leqslant p'$, d'où

$$(a^n)^p = (a^{-n'})^{-p'} = \left(\frac{1}{a^{n'}}\right)^{-p'} = (a^{n'})^{p'} = a^{(-n)(-p)} = a^{np}$$

en appliquant la formule (4).

Théorème.

Quels que soient a et b de $\mathbb{R}^*$ et n et p de $\mathbb{Z}$ on a

(1′) $\quad a^{n+p} = a^n a^p$

(2′) $\quad (ab)^n = a^n b^n$

(3′) $\quad (a^n)^p = a^{np}$.

REMARQUE

2. Dans tout anneau unitaire A on posera, pour tout $a \neq 0_A$, $a^0 = e$.

   Dans tout corps K on posera pour tout $a \neq 0_K$ et tout n de $\mathbb{N}^*$, $a^{-n} = \frac{1}{a^n}$.

   Les formules (1′) et (3′) sont vraies dans tout corps; la formule (2′) est vraie dans tout corps commutatif.

EXERCICE

2. Démontrer que quels que soient a et b de $\mathbb{R}^*$ et n et p de $\mathbb{Z}$ on a

$$\frac{a^n}{a^p} = a^{n-p} \quad \text{et} \quad \left(\frac{a}{b}\right)^n = \frac{a^n}{b^n}.$$

c) Puissances entières et ordre.

Les propriétés du produit (en particulier l'axiome **OM**) montrent que quels que soient a de $\mathbb{R}^*$ et n de $\mathbb{Z}$ on a

$$0 < a \Longrightarrow 0 < a^n,$$
$$a < 0 \Longrightarrow 0 < a^{2n},$$
$$a < 0 \Longrightarrow a^{2n+1} < 0.$$

Plus généralement étant donnés a et b de $\mathbb{R}$ cherchons à comparer a^n et b^n. Nous démontrerons d'abord le lemme suivant.

Lemme.

Quels que soient les nombres réels a et b et l'entier $n \geqslant 2$ on a

(5) $\quad a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$.

La formule est vraie pour $n = 2$

$$(a^2 - b^2) = (a - b)(a + b).$$

Supposons-la vraie pour $n \geqslant 2$; on a

$$\begin{aligned} a^{n+1} - b^{n+1} &= a^{n+1} - ab^n + ab^n - b^{n+1} \\ &= a(a^n - b^n) + (a - b)b^n \\ &= a(a - b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1}) + (a - b)b^n \\ &= (a - b)(a^n + a^{n-1}b + \ldots + a^2b^{n-2} + ab^{n-1} + b^n). \end{aligned}$$

La formule est donc vraie pour tout entier $n \geqslant 2$.

Étude dans $\mathbb{R}_+$.

Supposons $0 \leqslant a < b$ la formule (5) montre que $a^n < b^n$ pour $n \geqslant 2$; en effet $(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$ est un nombre strictement positif.
Pour $n = 1$, $a < b$ implique aussi $a^1 < b^1$.
Réciproquement si $a^n < b^n$ $(0 \leqslant a, 0 \leqslant b, 0 < n)$ on ne peut avoir ni $a = b$ (on aurait $a^n = b^n$), ni $b < a$ (on aurait $b^n < a^n$); concluons

Théorème.

Quels que soient les réels **positifs** a et b et l'entier naturel **non nul** n on a

$$(a < b) \iff (a^n < b^n)$$
$$(a = b) \iff (a^n = b^n).$$

Soit a un réel tel que $0 < a < 1$ pour tout n de $\mathbb{N}^*$ on aura $a^n < 1$ et pour tout entier n strictement négatif $a^n = \dfrac{1}{a^{-n}} > 1$.

Soit a un réel **strictement positif** et **distinct** de 1 tel que $a^n = 1$ $(n \in \mathbb{Z})$. On aura *ou bien* $0 < a < 1$ *ou bien* $1 < a$; dans les deux cas quel que soit l'entier relatif $n \neq 0$ on aura $a^n \neq 1$; comme $a^0 = 1$ nous pouvons énoncer :
Pour tout réel strictement positif distinct de 1 *et pour tout entier relatif n on a*

$$(a^n = 1) \iff (n = 0).$$

EXERCICE

3. Démontrer que l'application p

$$\begin{aligned} p : \mathbb{R}_+ &\longrightarrow \mathbb{R}_+ \\ x &\longmapsto x^n \end{aligned}$$

est strictement croissante pour $n > 0$ et strictement décroissante pour $n < 0$.

Étude dans $\mathbb{R}$.

Les résultats sont moins simples; en utilisant le théorème ci-dessus on peut cependant énoncer les résultats suivants :

Quels que soient a et b de $\mathbb{R}$ et n de $\mathbb{N}^*$ on a

$$|a| < |b| \iff |a|^n < |b|^n.$$

Quels que soient a et b de $\mathbb{R}^*$ et n de $\mathbb{Z}$ on a

$$|a| = |b| \iff |a|^n = |b|^n.$$

Soit a un nombre réel *non nul et distinct de* 1 *et* -1 vérifiant $a^n = 1$ $(n \in \mathbb{Z})$. On aura

$|a|^n = 1$, comme $|a| > 0$ et $|a| \neq 1$; on déduit du résultat obtenu ci-dessus que $n = 0$; concluons :

Théorème.

Pour tout nombre réel a distinct de 0, 1 et -1 on a

$$(a^n = 1) \iff (n = 0).$$

EXERCICE

4. Démontrer que l'application q

$$\begin{aligned} q : \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^{2n+1} \end{aligned}$$

est strictement croissante pour tout entier naturel n. Démontrer que l'application r

$$\begin{aligned} r : \mathbb{R}_- &\longrightarrow \mathbb{R}_+ \\ x &\longmapsto x^{2n} \end{aligned}$$

est strictement décroissante pour tout entier naturel $n \neq 0$.

d) Groupe des puissances entières d'un nombre réel non nul.

Soit a un élément quelconque de $\mathbb{R}^*$; désignons par $\mathbf{E}_a$ l'ensemble des puissances a^n où n est un entier relatif quelconque

$$\mathbf{E}_a = \{\ldots a^{-n}, \ldots, a^{-2}, a^{-1}, a^0 = 1, a^1, a^2, \ldots, a^n \ldots\}.$$

Cet ensemble $\mathbf{E}_a$ est une partie non vide du groupe multiplicatif $\mathbb{R}^*$; or quels que soient a^p et a^q de $\mathbf{E}_a$ on a

$$a^p (a^q)^{-1} = a^p a^{-q} = a^{p-q} \in \mathbf{E}_a.$$

Donc $(\mathbf{E}_a, \times)$ est un **sous-groupe** du groupe $(\mathbb{R}^*, \times)$; on l'appelle le **groupe des puissances entières de** $a \neq 0$.

Si $a = 1$, pour tout $n \in \mathbb{Z}$ on a $a^n = 1$; donc $\mathbf{E}_1 = \{1\}$; c'est le sous-groupe trivial réduit à l'élément neutre du groupe $(\mathbb{R}^*, \times)$.
Si $a = -1$, pour tout n de $\mathbb{Z}$ on a $a^n = 1$ (n pair) ou $a^n = -1$ (n impair); donc $\mathbf{E}_{-1} = \{1, -1\}$.
Supposons maintenant $a \neq 0$ et $|a| \neq 1$ et considérons l'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbf{E}_a \\ n &\longmapsto a^n. \end{aligned}$$

D'après la définition de $\mathbf{E}_a$ elle est *surjective*.
D'autre part quels que soient p et q de $\mathbb{Z}$ on a

$$(a^p = a^q) \iff (a^{p-q} = 1) \iff (p - q = 0)$$

puisque $a \neq 0$, $a \neq 1$ et $a \neq -1$; l'application f est donc *injective*. C'est donc une **bijection.**
D'autre part quels que soient p et q de $\mathbb{Z}$ on a $a^{p+q} = a^p a^q$,
c'est-à-dire $f(p + q) = f(p) f(q)$;

nous pouvons donc énoncer :

Théorème.

Pour tout nombre réel a **distinct de** 0, 1 **et** -1 l'application

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow \mathbf{E}_a \\ n &\longmapsto a^n \end{aligned}$$

définit un isomorphisme du groupe $(\mathbb{Z}, +)$ sur le groupe $(\mathbf{E}_a, \times)$.

3. 10 IDENTITÉS REMARQUABLES. FORMULE DU BINOME

a) Nous avons vu au § 3.9 c que quels que soient les nombres réels x et y et l'entier naturel $n \geqslant 2$ on a

$$\boxed{x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})}$$

Une telle égalité, vraie quels que soient x et y de $\mathbb{R}$ est appelée *identité*. Vous retrouvez en particulier les identités que vous connaissez déjà

$$x^2 - y^2 = (x - y)(x + y),$$
$$x^3 - y^3 = (x - y)(x^2 + xy + y^2).$$

EXERCICE

1. En changeant y en $-y$ dans l'identité précédente et en supposant n impair montrer que l'on a

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1});$$

en particulier

$$x^3 + y^3 = (x + y)(x^2 - xy + y^2),$$
$$x^5 + y^5 = (x + y)(x^4 - x^3y + x^2y^2 - xy^3 + y^4).$$

b) **Formule du binôme.**

Nous allons calculer $(x + y)^n$ quels que soient x et y de $\mathbb{R}$ et n de $\mathbb{N}^*$ comme somme de nombres réels de la forme ax^py^q où a, p, q sont des entiers naturels. Vous savez que l'on a

$$(x + y)^2 = x^2 + 2xy + y^2$$
$$(x + y)^3 = x^3 + 3xy^2 + 3x^2y + y^3$$

en joignant à ces exemples $(x + y)^1 = 1x^1 + 1y^1$ et en utilisant les coefficients binomiaux (cf. § 1.8 d) nous voyons que l'on peut écrire

$$(x + y)^1 = C_1^0 x^1 + C_1^1 y^1,$$
$$(x + y)^2 = C_2^0 x^2 + C_2^1 x^1 y^1 + C_2^2 y^2,$$
$$(x + y)^3 = C_3^0 x^3 + C_3^1 x^2 y^1 + C_3^2 x^1 y^2 + C_3^3 y^3.$$

Supposons, hypothèse de récurrence, que la formule

(B) $$(x + y)^n = C_n^0 x^n + \ldots + C_n^h x^{n-h} y^h + \ldots + C_n^n y^n$$

soit vraie pour l'entier $n \geqslant 1$. Nous allons montrer qu'elle est encore vraie pour $n + 1$. Quels que soient x et y de $\mathbb{R}$ on a

$$(x + y)^{n+1} = (x + y)^n (x + y).$$

Les termes de $(x + y)^{n+1}$ sont donc obtenus en multipliant chaque terme $C_n^h x^{n-h} y^h$ $(0 \leqslant h \leqslant n)$ de $(x + y)^n$ par x puis par y. Nous obtiendrons donc des termes de la forme ax^py^q $(a, p, q \in \mathbb{N})$ avec $p + q = n + 1$.
Le terme en x^{n+1} de $(x + y)^{n+1}$ est unique c'est

$$(C_n^0 x^n)\, x = C_n^0 x^{n+1} = x^{n+1} = C_{n+1}^0 x^{n+1}$$

car $C_n^0 = C_{n+1}^0 = 1$.
Il en est de même du terme en y^{n+1}, c'est

$$(C_n^n y^n)\, y = C_n^n y^{n+1} = y^{n+1} = C_{n+1}^{n+1} y^{n+1}.$$

Considérons le terme en $x^{n+1-h}y^h$ $(1 \leqslant h \leqslant n)$ de $(x+y)^{n+1}$ il est obtenu de deux façons :

- soit en multipliant par x le terme en $x^{n-h}y^h$ de $(x+y)^n$,
- soit en multipliant par y le terme en $x^{n-(h-1)}y^{h-1}$ de $(x+y)^n$.

Le terme en $x^{n+1-h}y^h$ $(1 \leqslant h \leqslant n)$ de $(x+y)^{n+1}$ est donc

$$(C_n^h x^{n-h}y^h)\,x + (C_n^{h-1}x^{n-(h-1)}y^{h-1})\,y$$
$$= (C_n^{h-1} + C_n^h)\,x^{n+1-h}y^h = C_{n+1}^h x^{n+1-h}y^h,$$

car (cf. § 1.) $C_n^{h-1} + C_n^h = C_{n+1}^h$. On a donc

$$(x+y)^{n+1} = C_{n+1}^0 x^{n+1} + \ldots + C_{n+1}^h x^{n+1-h}y^h + \ldots + C_{n+1}^{n+1}y^{n+1}.$$

La formule étudiée est vraie pour $n = 1$; si elle est vraie pour n, alors elle est vraie pour $n+1$: elle est donc vraie pour tout entier naturel non nul.

Théorème.

Quels que soient les nombres réels x et y et quel que soit l'entier naturel non nul n on a la formule appelée **formule du binôme.**

$$(x+y)^n = C_n^0 x^n + \ldots + C_n^h x^{n-h}y^h + \ldots + C_n^n y^n$$

Cette formule du *binôme* $(x+y$ a deux termes, c'est un binôme) explique la dénomination « *coefficients binomiaux* » donnés aux entiers naturels de la forme C_n^p.
Rappelons que l'on a

$$C_n^p = \frac{n(n-1)\ldots(n-p+1)}{p!} = \frac{n!}{p!\,(n-p)!}.$$

REMARQUES

1. Si $x \neq 0$, $y \neq 0$, $x+y \neq 0$ la formule est encore valable pour $n = 0$, en effet dans ce cas
$$(x+y)^0 = 1 = C_0^0 x^0 y^0$$
et les coefficients des binômes successifs $n = 0, 1\ldots$ sont les éléments du triangle de Pascal

1					
1	1				
1	2	1			
1	3	3	1		
1	4	6	4	1	
1	5	10	10	5	1
.....					

2. La démonstration de la formule du binôme dans $\mathbb{R}$, n'utilise pas l'axiome $\mathbf{M_3}$ (tout élément *non nul* de $\mathbb{R}$ a un inverse) mais uniquement les propriétés de $\mathbb{R}$ considéré comme anneau commutatif.
La formule du binôme $(n \geqslant 1)$ s'applique donc dans tout anneau commutatif : il suffit de définir pour tout x de l'anneau commutatif A et tout *entier* $n \geqslant 1$ les éléments x^n et nx de l'anneau A. En posant
$$x^1 = x \quad \text{et} \quad x^{n+1} = x^n.x$$
$$1\,x = x \quad \text{et} \quad (n+1)\,x = nx + x$$
on vérifie sans peine que quels que soient p et q de $\mathbb{N}^*$ on a
$$x^p x^q = x^{p+q} \quad , \quad (p+q)\,x = px + qx.$$
Vous constaterez que ces propriétés jointes aux propriétés de l'addition et de la multiplication dans l'anneau commutatif A vous permettent de répéter mot pour mot dans tout anneau commutatif A la démonstration faite ci-dessus dans $\mathbb{R}$.

EXERCICES

2. En faisant $x = y = 1$ dans la formule du binôme, calculer $C_n^0 + C_n^1 + \ldots + C_n^n$
En faisant $x = 1$ et $y = -1$ calculer

$$P = C_n^0 + C_n^2 + C_n^4 + \ldots .$$
$$I = C_n^1 + C_n^3 + C_n^5 + \ldots .$$

(le dernier terme n'a pas été écrit dans P et I car sa forme dépend de la parité de n).

3. Dans la formule $(x+1)^2 = x^2 + 2x + 1$ faire successivement $x = 1, 2, \ldots, n \in \mathbb{N}^*$ et additionner les égalités obtenues. En déduire pour tout $n \in \mathbb{N}^*$

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2}.$$

4. Dans la formule $(x+1)^3 = x^3 + 3x^2 + 3x + 1$ faire successivement $x = 1, 2, \ldots, n \in \mathbb{N}^*$ et additionner les égalités obtenues. En déduire — en utilisant le résultat de l'exercice 3 — que pour tout $n \in \mathbb{N}^*$ on a

$$1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

III. Conséquences de l'ensemble des axiomes définissant $\mathbb{R}$

3. 11 BORNE SUPÉRIEURE ET BORNE INFÉRIEURE

a) Axiome de la borne supérieure et premières conséquences.

Rappelons l'axiome **BS**.

BS. Toute partie non vide majorée de $\mathbb{R}$ a une borne supérieure dans $\mathbb{R}$.

Une partie A de $\mathbb{R}$ est *majorée* si l'ensemble des *majorants* de A n'est pas vide, c'est-à-dire s'il existe $a \in \mathbb{R}$ tel que

$$(\forall\, x \in A) \quad x \leqslant a.$$

La *borne supérieure* est alors *le plus petit des majorants* et on écrit

$$\alpha = \sup A.$$

Maintenant que nous avons défini $\mathbb{Q}$ (cf. § 3.7) nous pourrions reprendre, dans la suite logique de notre exposé, ce que nous avons montré au § 3.1, à savoir qu'il existe dans $\mathbb{Q}$ des parties non vides majorées n'ayant pas de borne supérieure dans $\mathbb{Q}$.
La propriété **BS** étant vraie dans $\mathbb{R}$ et non dans $\mathbb{Q}$ il en résulte que $\mathbb{Q} \neq \mathbb{R}$ c'est-à-dire que $\mathbb{Q}$ est une **partie stricte** de $\mathbb{R}$. Les nombres réels non rationnels sont appelés nombres **irrationnels.**

Soit d'autre part une partie non vide, minorée A de $\mathbb{R}$. L'ensemble $-A$ des opposés des éléments de A est une partie non vide majorée de $\mathbb{R}$; $-A$ a donc une borne supérieure que nous notons $-\alpha$; ce nombre réel $-\alpha$ est donc *le plus petit des majorants* de $-A$. Les propriétés de la relation $\leqslant$ dans $\mathbb{R}$ montrent que α est le *plus grand des minorants* de A, c'est-à-dire que A a une borne inférieure dans $\mathbb{R}$. Concluons

Toute partie non vide minorée de $\mathbb{R}$ a une borne inférieure dans $\mathbb{R}$.

On écrira

$$\alpha = \inf A.$$

Si une partie non vide A de $\mathbb{R}$ est *bornée*, c'est-à-dire *majorée* et *minorée*, il existe des nombres réels α et β tels que

$$\alpha = \inf A \quad \text{et} \quad \beta = \sup A.$$

Comme pour tout a de A on a, $\alpha \leqslant a$ et $a \leqslant \beta$, il en résulte que $\alpha \leqslant \beta$.

b) Caractérisation de la borne supérieure et de la borne inférieure.

Soit α la borne supérieure de A partie non vide majorée de $\mathbb{R}$; α étant un majorant de A on a

(1) $$(\forall\, a \in A) \qquad a \leqslant \alpha.$$

D'autre part α est *le plus petit des majorants* de A; donc si β est un nombre réel strictement inférieur à α mais, par ailleurs quelconque, il existe au moins un élément b de A tel que $\beta < b \leqslant \alpha$. En effet s'il n'existait pas au moins un tel b de A, *tous* les éléments de A seraient inférieurs à β et β serait un majorant de A strictement inférieur à α, ce qu est impossible; on a donc

$$(\forall\, \beta \in]-\infty, \alpha[) \quad (\exists\, b \in A) \qquad \beta < b.$$

Le nombre $\beta < \alpha$ peut s'écrire $\beta = \alpha - \varepsilon$ ou ε est un élément quelconque de $\mathbb{R}_+^*$; la borne supérieure α vérifie donc la propriété

(2) $$(\forall\, \varepsilon \in \mathbb{R}_+^*) \quad (\exists\, b \in A) \qquad \alpha - \varepsilon < b.$$

Réciproquement soit A une partie non vide de $\mathbb{R}$ et un nombre réel α tels que l'on ait (1) et (2). D'après (1) A est majorée et α est un majorant; d'autre part (2) implique que α est le plus petit des majorants de A; en effet s'il existait un majorant α' de A tel que $\alpha' < \alpha$, en appliquant la propriété (2) avec $\varepsilon < \alpha - \alpha'$ on mettrait en évidence un élément b de A tel que $\alpha' < b$, ce qui est faux puisque α' est supposé être un majorant de A. Concluons :

Théorème.

Quels que soient la partie non vide A de $\mathbb{R}$ et le nombre réel α, les propriétés suivantes sont équivalentes.

i) $\alpha = \sup A$

ii) 1. $(\forall\, a \in A) \quad a \leqslant \alpha,$
et
2. $(\forall\, \varepsilon \in \mathbb{R}_+^*) \; (\exists\, b \in A) \quad \alpha - \varepsilon < b.$

Vous démontrerez de même

Quels que soient la partie non vide A de $\mathbb{R}$ et le nombre réel α, les propriétés suivantes sont équivalentes.

i) $\alpha = \inf A$

ii) 1. $(\forall\, a \in A) \quad \alpha \leqslant a,$
et
2. $(\forall\, \varepsilon \in \mathbb{R}_+^*) \; (\exists\, b \in A) \quad b < \alpha + \varepsilon.$

EXEMPLES

1. Considérons l'ensemble A des nombres réels de la forme

$$u_n = \frac{1}{n} + (-1)^n$$

où n est un entier naturel non nul quelconque. On voit que l'on a

$$u_{2p} = 1 + \frac{1}{2p} \qquad (p > 0),$$

$$u_{2q+1} = -1 + \frac{1}{2q+1} \qquad (q \geqslant 0).$$

Ces nombres sont indiqués sur la figure 1.

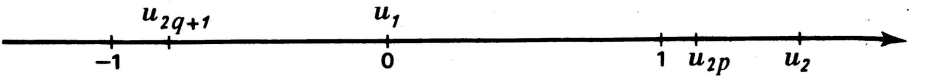


fig. 1

On voit que pour tout élément u_n de A on a

$$-1 \leqslant u_n \leqslant \frac{3}{2};$$

donc l'ensemble A est *borné*, c'est-à-dire à la fois *majoré* et *minoré*.

Le nombre réel $u_2 = 1 + \frac{1}{2} = \frac{3}{2}$ est le plus grand élément de l'ensemble A, c'est donc le plus petit majorant de A, c'est-à-dire la borne supérieure de A; on a dans ce cas

$$\sup A = \frac{3}{2} \quad \text{et} \quad \frac{3}{2} \in A.$$

On voit aussi que quel que soit ε de $\mathbb{R}_+^*$ pour avoir

$$u_{2q+1} < -1 + \varepsilon$$

il suffit de prendre $2q + 1 > \frac{1}{\varepsilon}$ ce qui est toujours possible; donc -1 est la borne inférieure de A; on constate que $-1 \notin A$; donc, dans ce cas on a

$$\inf A = -1 \quad \text{et} \quad -1 \notin A.$$

Si on considérait l'ensemble B des nombres réels de la forme

$$v_n = -\frac{1}{n} + (-1)^{n+1}$$

où n est un entier naturel non nul quelconque on constaterait

$$\sup B = 1 \quad \text{et} \quad 1 \notin B,$$

$$\inf B = -\frac{3}{2} \quad \text{et} \quad -\frac{3}{2} \in B.$$

2. Si A possède un plus grand élément cet élément est sup A; de même si A possède un plus petit élément cet élément est inf A. Cela se produit toujours pour A *fini*; si A comprend $n > 0$ nombres réels

$$a_1 < a_2 \ldots < a_n$$

on a

$$\inf A = a_1 \quad \text{et} \quad \sup A = a_n.$$

Ces exemples montrent que la borne supérieure (ou la borne inférieure) d'un ensemble A, lorsqu'elle existe, **peut appartenir** ou **ne pas appartenir à** A.

REMARQUE

Si $\alpha = \sup A$ appartient à A il peut arriver, comme dans l'exemple ci-dessus, que pour certaines valeurs de $\varepsilon > 0$ le seul élément b de A tel que $\alpha - \varepsilon < b \leqslant \alpha$ soit α lui-même. Dans l'exemple ci-dessus on a pour les éléments strictement positifs de A

$$u_{2p} < \ldots < u_4 < u_2$$

avec $u_4 = 1 + \frac{1}{4} = \frac{5}{4}$, $u_2 = 1 + \frac{1}{2} = \frac{3}{2} = \sup A$; si on prend $\varepsilon < \frac{3}{2} - \frac{5}{4} = \frac{1}{4}$ le seul b de A tel que $\frac{3}{2} - \varepsilon < b \leqslant \frac{3}{2}$ est $\frac{3}{2} = \sup A$.

3.12 CARACTÉRISATION DES INTERVALLES DE $\mathbb{R}$

Rappelons (cf. § 3.6 a) que l'on appelle *intervalle* de $\mathbb{R}$ l'une quelconque des parties de $\mathbb{R}$ suivantes ($a \in \mathbb{R}$, $b \in \mathbb{R}$, $a \leqslant b$)

$$[a, b] \ , \ ]a, b[\ , \ [a, b[\ , \ ]a, b],$$
$$]-\infty, b] \ , \ ]-\infty, b[\ , \ [a, +\infty[\ , \ ]a, +\infty[,$$
$$]-\infty, +\infty[= \mathbb{R}.$$

Toutes ces parties sont *non vides* sauf $]a, a[$, $[a, a[$, $]a, a]$.
Pour tout intervalle I de $\mathbb{R}$, quels que soient x et y de $\mathbb{R}$ appartenant à I et vérifiant $x \leqslant y$ on a

$$[x, y] \subset \mathrm{I}.$$

Considérons, *réciproquement*, une partie P non vide de $\mathbb{R}$ telle que, quels que soient x et y de P ($x \leqslant y$), on ait $[x, y] \subset \mathrm{P}$.

Premier cas : P est *bornée*. P non vide est donc majorée et minorée, il existe donc α et β de $\mathbb{R}$ tels que

$$\alpha = \inf A, \qquad \beta = \sup A \quad \text{avec} \quad \alpha \leqslant \beta;$$

et on a

$$\mathrm{P} \subset [\alpha, \beta].$$

Si $\alpha = \beta$ la partie P (non vide) ne peut être que $[\alpha, \alpha]$, donc P est un intervalle non vide.
Si $\alpha < \beta$ considérons un réel quelconque r vérifiant $\alpha < r < \beta$; d'après une propriété de la borne supérieure (ou de la borne inférieure) il existe x et y de P tels que

$$\alpha \leqslant x < r < y \leqslant \beta.$$

Il en résulte que $r \in \mathrm{P}$ puisque, d'après l'hypothèse faite sur P, on a $[x, y] \subset \mathrm{P}$.
Donc tout réel r tel que $\alpha < r < \beta$ appartient à P c'est-à-dire

$$]\alpha, \beta[\subset \mathrm{P}.$$

D'autre part on a $\mathrm{P} \subset [\alpha, \beta]$, par conséquent on ne peut avoir que l'un des 4 cas suivants :

$$\mathrm{P} = [\alpha \ , \beta] \quad \text{ou} \quad \mathrm{P} =]\alpha \ , \beta[\quad \text{ou} \quad \mathrm{P} = [\alpha \ , \beta[\quad \text{ou} \quad \mathrm{P} =]\alpha \ , \beta],$$

selon que α ou β appartient ou non à P. Donc P est encore un intervalle non vide ($\alpha < \beta$).

Deuxième cas : P non vide est *majorée, non minorée*. Il existe donc β de $\mathbb{R}$ tel que

$$\beta = \sup P$$

et on a

$$P \subset]-\infty\ ,\ \beta].$$

Soit r un réel quelconque vérifiant $r < \beta$; il existe y de P tel que

$$r < y \leqslant \beta;$$

de plus il existe x de P tel que

$$x < r;$$

en effet, s'il n'existait pas un tel x dans P, cela voudrait dire que pour tout x de P on aurait $r \leqslant x$ et P serait minorée.
Il existe donc x et y de P tels que

$$x < r < y \leqslant \beta.$$

Il en résulte que $r \in P$ puisque, d'après l'hypothèse faite $[x\ ,\ y] \subset P$. Donc tout réel r tel que $r < \beta$ appartient à P c'est-à-dire

$$]-\infty\ ,\ \beta[\subset P.$$

D'autre part on a $P \subset]-\infty\ ,\ \beta]$, par conséquent on ne peut avoir que l'un des cas suivants :

$$P =]-\infty\ ,\ \beta] \quad \text{ou} \quad P =]-\infty\ ,\ \beta[,$$

selon que $\beta = \sup P$ appartient ou non à P. Donc P est encore un intervalle non vide de $\mathbb{R}$.

Troisième cas : P non vide est *minorée* et non *majorée*. Vous démontrerez de même, en posant $\alpha = \inf P$, que l'on a nécessairement

$$P = [\alpha\ ,\ +\infty[\quad \text{ou} \quad P =]\alpha\ ,\ +\infty[;$$

P est donc encore un intervalle non vide de $\mathbb{R}$.

Quatrième cas : P est *non minorée* et *non majorée*. Quel que soit r de $\mathbb{R}$ il existe x et y de $\mathbb{R}$ tels que

$$x < r \quad \text{et} \quad r < y,$$

sinon la partie P serait majorée ou minorée; donc

$$x < r < y$$

et d'après l'hypothèse faite ($[x\ ,\ y] \subset P$ si x et y appartiennent à P) on a $r \in P$. Donc tout réel r appartient à P, c'est-à-dire, puisque $P \subset \mathbb{R}$, on a

$$P =]-\infty\ ,\ +\infty[= \mathbb{R}.$$

Concluons

Théorème.

Une partie non vide P de $\mathbb{R}$ est un intervalle non vide de $\mathbb{R}$ si et seulement si quels que soient x et y de P vérifiant $x \leqslant y$ on a $[x\ ,\ y] \subset P$.

EXERCICE

Soient deux intervalles I et I′ de $\mathbb{R}$; démontrer que si $I \cap I' \neq \varnothing$ alors $I \cap I'$ est un intervalle.

3. 13 PARTIES ADJACENTES DE $\mathbb{R}$. APPLICATIONS

a) Parties adjacentes de $\mathbb{R}$.

Soient A et A′ deux parties non vides de $\mathbb{R}$ telles que

$$\sup A = \inf A'.$$

Désignons par α cette borne commune; quels que soient x de A et x' de A′ on a

$$x \leqslant \alpha \leqslant x';$$

d'où

(1) $$(\forall\, x \in A) \quad (\forall\, x' \in A') \qquad x \leqslant x'.$$

D'autre part quel que soit $\varepsilon > 0$ il existe y de A et y' de A′ tels que

$$\alpha - \varepsilon < y \leqslant \alpha \leqslant y' < \alpha + \varepsilon;$$

d'où

$$0 \leqslant y' - y < [\alpha + \varepsilon - (\alpha - \varepsilon)] = 2\varepsilon.$$

Si nous remplaçons ε par $\frac{\varepsilon}{2}$, ce nombre $\frac{\varepsilon}{2}$ est encore un réel strictement positif quelconque et nous avons

(2) $$(\forall\, \varepsilon \in \mathbb{R}_+^*) \quad (\exists\, y \in A) \quad (\exists\, y' \in A') \qquad |y' - y| < \varepsilon.$$

Réciproquement soient A et A′ deux parties non vides de $\mathbb{R}$ vérifiant les propriétés (1) et (2).

D'après (1) A non vide est majorée par n'importe quel élément x' de A′; de même A′, non vide, est minorée par n'importe quel élément x de A; il existe donc des nombres réels α et α' tels que

$$\sup A = \alpha \quad \text{et} \quad \inf A = \alpha'.$$

Nous allons montrer que $\alpha = \alpha'$.

Si $\alpha < \alpha'$, *quels que soient* $x \in A$ et $x' \in A'$ on a

$$x \leqslant \alpha < \alpha' \leqslant x';$$

donc $0 < \alpha' - \alpha \leqslant x' - x$; et, par conséquent si on prend par exemple $\varepsilon < \frac{\alpha' - \alpha}{2}$ il sera impossible de trouver $y \in A$ et $y' \in A'$ vérifiant $y' - y < \varepsilon$; la relation (2) ne sera pas vérifiée. Donc $\alpha < \alpha'$ est impossible.

Si $\alpha' < \alpha$ prenons ε tel que $\varepsilon < \frac{\alpha - \alpha'}{2}$, il existe $x \in A$ et $x' \in A'$ tels que

$$\alpha - \varepsilon < x \leqslant \alpha \quad \text{et} \quad \alpha' \leqslant x' < \alpha' + \varepsilon.$$

Or $\alpha - \varepsilon - (\alpha' + \varepsilon) = \alpha - \alpha' - 2\varepsilon > 0$, on a donc (fig. 2)

$$x' < \alpha' + \varepsilon < \alpha - \varepsilon < x$$

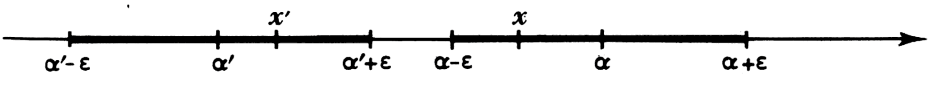


fig. 2

ce qui est impossible d'après (1). Donc $\alpha' < \alpha$ est impossible. Concluons :

Théorème et définition.

Quelles que soient les parties non vides A et A′ de $\mathbb{R}$ les propriétés suivantes sont équivalentes

i) $\sup A = \inf A'$

ii) $\begin{cases} (1) \quad (\forall\, x \in A) \quad (\forall\, x' \in A') \qquad x \leqslant x' \\ \qquad\qquad \text{et} \\ (2) \quad (\forall\, \varepsilon \in \mathbb{R}_+^*) \quad (\exists\, y \in A) \quad (\exists\, y' \in A') \qquad |y' - y| < \varepsilon. \end{cases}$

Tout couple de parties non vides de $\mathbb{R}$ vérifiant la propriété *i* ou la propriété *ii* est appelé couple de **parties adjacentes** de $\mathbb{R}$.

Le nombre réel $\alpha = \sup A = \inf A'$ est le **seul nombre réel** vérifiant

$$(\forall\, x \in A)\,(\forall\, x' \in A') \qquad x \leqslant \alpha \leqslant x'.$$

EXEMPLE

L'ensemble A des nombres réels de la forme $1 - \frac{1}{n}$ et l'ensemble A′ des nombres réels de la forme $1 + \frac{1}{n}$ où n est un entier naturel non nul quelconque définissent deux parties adjacentes de $\mathbb{R}$.

Dans les paragraphes suivants nous rencontrerons de nombreux exemples de parties adjacentes de $\mathbb{R}$.

Chacune des conditions *i* et *ii* ci-dessus est une condition nécessaire et suffisante pour que A et A′ soient des parties adjacentes de $\mathbb{R}$. Voici une condition *suffisante* qui rend des services dans les applications.

Considérons deux parties non vides A et A′ de $\mathbb{R}$ possédant les propriétés suivantes

(1) $\qquad (\forall\, x \in A) \quad (\forall\, x' \in A') \qquad x \leqslant x'$,

(2′) $\qquad A \cup A'$ est un intervalle de $\mathbb{R}$.

Comme dans la réciproque ci-dessus on montrera que A est majorée et A′ minorée et donc qu'il existe α et α' tels que $\alpha = \sup A$ et $\alpha' = \inf A'$; toujours comme dans cette réciproque on montrera que $\alpha' < \alpha$ est impossible.

Si $\alpha < \alpha'$ on aura pour tout x de A et tout x' de A′

$$x \leqslant \alpha < \alpha' \leqslant x'$$

et tous les éléments de $]\alpha, \alpha'[$, qui n'est pas vide, n'appartiendront pas à $A \cup A'$ qui par conséquent ne sera pas un intervalle (cf § 3.12); donc $\alpha < \alpha'$ est aussi impossible. Concluons :

Tout couple de parties non vides A et A′ de $\mathbb{R}$ vérifiant

$$\begin{cases} (1) \quad (\forall\, x \in A) \quad (\forall\, x' \in A') \qquad x \leqslant x', \\ \qquad\qquad \text{et} \\ (2') \quad A \cup A' \text{ est un intervalle de } \mathbb{R}, \end{cases}$$

est un couple de parties adjacentes de $\mathbb{R}$.

b) Propriétés des segments emboîtés.

A tout entier naturel n associons un *intervalle fermé* $S_n = [a_n, b_n]$ de $\mathbb{R}$; on a donc, pour tout n de $\mathbb{N}$, $a_n \leqslant b_n$. Nous définissons ainsi une *suite infinie d'intervalles fermés* — on dit aussi une *suite infinie de segments*.

Nous supposons d'abord que pour tout n de $\mathbb{N}$

(1) $$S_{n+1} \subset S_n$$

on en déduit immédiatement par récurrence sur k que quels que soient n et k de $\mathbb{N}$

$$S_{n+k} \subset S_n$$

c'est-à-dire que, quels que soient p et q de $\mathbb{N}$, on a

$$(p \leqslant q) \Longrightarrow (S_q \subset S_p).$$

Si nous désignons par $\mathcal{S}$ l'ensemble des segments S_n où n est un entier naturel quelconque, l'application

$$\begin{aligned} f : \mathbb{N} &\longrightarrow \mathcal{S} \\ n &\longmapsto S_n \end{aligned}$$

est telle que quels que soient p et q de $\mathbb{N}$

$$(p \leqslant q) \Longrightarrow (f(q) \subset f(p)) \ ;$$

c'est-à-dire l'application f, considérée comme application de $(\mathbb{N}, \leqslant)$ dans $(\mathcal{S}, \subset)$, est une **application décroissante.**

Considérons deux quelconques des segments précédents S_p et S_q $(p \leqslant q)$ la condition $S_p \subset S_q$ s'écrit

$$a_q \leqslant a_p \leqslant b_p \leqslant b_q.$$

Donc $a_p \leqslant b_q$ et $a_q \leqslant b_q$. On a donc

(1) $$(\forall\, p \in \mathbb{N}) \quad (\forall\, q \in \mathbb{N}) \qquad a_p \leqslant b_q.$$

Supposons de plus que l'on ait

(2) $$(\forall\, \varepsilon \in \mathbb{R}_+^*) \quad (\exists\, p \in \mathbb{N}) \qquad b_p - a_p < \varepsilon.$$

Si nous posons

$$\begin{aligned} A &= \{a_0, a_1, \ldots, a_n, \ldots\}, \\ B &= \{b_0, b_1, \ldots, b_n, \ldots\}, \end{aligned}$$

les conditions (1) et (2) montrent que A et B sont *adjacentes* dans $\mathbb{R}$, il existe donc α de $\mathbb{R}$ tel que

$$\alpha = \sup A = \inf B.$$

Ce nombre α est le *seul nombre réel* tel que

$$(\forall\, n \in \mathbb{N}) \qquad a_n \leqslant \alpha \leqslant b_n.$$

Autrement dit l'intersection de *tous* les segments $S_n = [a_n, b_n]$ est $\{\alpha\}$, nous écrirons

$$\bigcap_{n \in \mathbb{N}} [a_n, b_n] = \{\alpha\}.$$

Théorème des segments emboîtés.

Pour toute suite infinie de segments $S_n = [a_n, b_n]$, où $a_n \leqslant b_n$, vérifiant les deux propriétés

(1) $(\forall\, n \in \mathbb{N}) \quad S_{n+1} \subset S_n$

(2) $(\forall\, \varepsilon \in \mathbb{R}_+^*) \quad (\exists\, p \in \mathbb{N}) \quad b_p - a_p < \varepsilon,$

il existe un nombre réel unique α appartenant à tous les segments S_n.

Les propriétés (1) et (2) sont appelées les conditions du théorème des segments emboîtés

REMARQUES

1. Nous venons de démontrer que l'axiome **BS** joint au fait que $(\mathbb{R}, +, \times, \leqslant)$ est un corps commutatif totalement ordonné entraîne la propriété **SE** des segments emboîtés; réciproquement on démontre que les propriétés de $(\mathbb{R}, +, \times, \leqslant)$ et la propriété **SE** entraîne la propriété **BS.** Cette démonstration étant beaucoup plus difficile que celle que nous avons faite (**BS** entraîne **SE**) nous avons préféré prendre pour axiome **BS** et non **SE.**
   En Seconde, en revanche, ne voulant pas introduire la notion de borne supérieure, nous avions pris la propriété **SE** comme axiome.
2. Le fait que les intervalles soient *fermés* est essentielle. Par exemple pour $]a_n, b_n]$ où $a_n = 0$ et $b_n = \frac{1}{n}$ on a $\sup A = \inf B = 0$ et 0 n'appartient à aucun des intervalles. Il en serait de même pour les intervalles $\left[\frac{1}{n}, 0\right[$.

c) Racine n$^{\text{ième}}$ positive d'un nombre réel positif.

Soit a un nombre réel positif quelconque et n un entier naturel $\geqslant 1$; nous cherchons un nombre réel positif x tel que $x^n = a$. Si un tel nombre existe, il est unique car nous avons vu que dans $\mathbb{R}_+$ la relation $x^n = x'^n$ est équivalente à $x = x'$.
Si $a = 0$ on a $x = 0$.
Supposons $a > 0$. Considérons les deux parties suivantes de $\mathbb{R}$

$$\begin{aligned} A &= \{x \in \mathbb{R}_+ \mid x^n \leqslant a\}, \\ A' &= \{x' \in \mathbb{R}_+ \mid a < x'^n\}. \end{aligned}$$

Le nombre 0 appartient à A donc A est non vide. Montrons que A′ comprend des nombres réels > 1; soit $x' = 1 + y'$ (avec $y' > 0$) un tel nombre; en appliquant la formule du binôme à $(1 + y')^n$ on obtient

$$x'^n = (1 + y')^n = 1 + C_n^1 y' + \ldots + C_n^h y'^h + \ldots + y'^n,$$

d'où

$$x'^n > ny',$$

tous les termes négligés étant strictement positifs; donc en prenant $ny' > a$ c'est-à-dire, par exemple $y' = \frac{a}{n} + 1$, le nombre $x' = 1 + y'$ est tel que $x'^n > a$.

Les parties A et A′ de $\mathbb{R}$ sont donc non vides.
Quels que soient x de A et x' de A′ on a

$$x^n \leqslant a < x'^n,$$

d'où $x^n < x'^n$; par conséquent, puisque x et x' appartiennent à $\mathbb{R}_+$, nous avons

(1) $\qquad (\forall\, x \in A) \quad (\forall\, x' \in A') \qquad x < x'.$

D'autre part, l'ordre étant total dans $\mathbb{R}$, quel que soit r de $\mathbb{R}_+$ on a $r^n \leqslant a$ ou $a < r^n$ c'est-à-dire

(2′) $\qquad A \cup A' = \mathbb{R}_+.$

Or $\mathbb{R}_+ = [0, +\infty[$ est un intervalle non vide de $\mathbb{R}$. Les parties non vides A et A′ de $\mathbb{R}$ vérifient donc les propriétés (1) et (2′); d'après un résultat vu plus haut ce sont deux parties non vides adjacentes. Posons

$$\alpha = \sup A = \inf A'.$$

Quels que soient x de A et x' de A′ nous avons $x \leqslant \alpha \leqslant x'$; d'où $x^n \leqslant \alpha^n \leqslant x'^n$.

Donc, quels que soient $x \in A$ et $x' \in A'$, on a

(3) $$x^n \leqslant \alpha^n \leqslant x'^n$$

et

(4) $$x^n \leqslant a < x'^n.$$

Nous allons montrer que $\alpha^n = a$. Considérons pour cela l'ensemble B de toutes les puissances $n^{\text{ièmes}}$ des éléments de A et l'ensemble B' de toutes les puissances $n^{\text{ièmes}}$ des éléments de A'; ces parties B et B' de $\mathbb{R}$ sont donc non vides et on a

$$B = \{y \in \mathbb{R}_+ \mid (\exists\, x \in A) \quad y = x^n\}$$
$$B' = \{y' \in \mathbb{R}_+ \mid (\exists\, x' \in A') \quad y' = x'^n\}$$

Nous allons montrer que B et B' sont adjacentes. Nous avons d'abord

$$(\forall\, y \in B) \quad (\forall\, y' \in B') \qquad y \leqslant y'.$$

Soit ε un nombre réel strictement positif quelconque, cherchons y de B et y' de B' tels que $|y' - y| < \varepsilon$. Nous avons (cf. § 3.10 a)

(5) $$y' - y = x'^n - x^n = (x' - x)(x'^{n-1} + x'^{n-2}x + \ldots + x'x^{n-2} + x^{n-1}).$$

Choisissons x'_0 dans A'; $0 < x_0$ car $0 < a < x'^n_0$. Quels que soient x de A et x' de A' vérifiant $x' \leqslant x'_0$ nous aurons, étant dans $\mathbb{R}_+$

(6) $$x'^n - x^n \leqslant (x' - x)\, n x'^{n-1}_0$$

car dans $x'^{n-1} + \ldots + x^{n-1}$ il y a n termes tous inférieurs à x'^{n-1}_0.
Les parties A et A' de $\mathbb{R}$ étant adjacentes il existe x_1 de A et x'_1 de A' tels que

$$x'_1 - x_1 \leqslant \frac{\varepsilon}{n x'^{n-1}_0}.$$

Si $x'_1 \leqslant x'_0$ posons $x'_2 = x'_1$; si $x'_0 < x'_1$ posons $x'_2 = x'_0$; dans les deux cas nous aurons

$$x'_2 - x_1 \leqslant \frac{\varepsilon}{n x'^{n-1}_0} \quad \text{et} \quad x'_2 \leqslant x'_0$$

donc d'après (5) et (6)

$$y'_2 - y_1 = x'^n_2 - x^n_1 \leqslant \varepsilon.$$

Donc B et B' sont deux parties adjacentes de $\mathbb{R}$.
Il existe donc un nombre réel unique $\beta = \sup B = \inf B'$ tel que quels que soient y de B et y' de B' on ait

$$y \leqslant \beta \leqslant y'.$$

Or d'après les relations (3) et (4) on a pour tout y de B et tout y' de B'

$$y \leqslant \alpha^n \leqslant y' \quad \text{et} \quad y \leqslant a \leqslant y'$$

donc

$$\alpha^n = a.$$

Théorème et définition.

Quel que soit le nombre réel positif a et quel que soit l'entier naturel non nul n il existe un nombre réel positif unique α tel que $\alpha^n = a$.

Ce nombre α est appelé **racine $n^{\text{ième}}$ positive** de a, il est noté $a^{\frac{1}{n}}$ ou $\sqrt[n]{a}$.

REMARQUE

3. Dans le tome 2 on donnera une autre démonstration de ce théorème en utilisant les propriétés de l'application $x \longmapsto x^n$ de $\mathbb{R}_+$ dans $\mathbb{R}_+$. On étudiera à ce moment les règles de calcul sur les radicaux et la résolution dans $\mathbb{R}$ de l'équation $x^n = a$ où a est un réel quelconque,

   Nous avons donné ici l'existence de $\sqrt[n]{a}$ pour $a \geqslant 0$ car nous en aurons besoin dans le chapitre 4 de ce tome 1 pour étudier les racines $n^{\text{ièmes}}$ d'un nombre complexe

3. 14 PROPRIÉTÉ D'ARCHIMÈDE ET APPLICATIONS

a) Propriété d'Archimède.

Quel que soit a de $\mathbb{R}$ il peut vous sembler « évident » qu'il existe un entier naturel n tel que $a < n$. Nous allons montrer cette propriété en utilisant les axiomes de $\mathbb{R}$. Considérons l'énoncé

$$\text{(P)} \qquad (\forall\, a \in \mathbb{R}) \quad (\exists\, n \in \mathbb{N}) \qquad a < n.$$

On aura, la négation de $a < n$ étant $n \leqslant a$

$$\text{(non P)} \qquad (\exists\, a \in \mathbb{R}) \quad (\forall\, n \in \mathbb{N}) \qquad n \leqslant a;$$

l'énoncé (non P) signifie que $\mathbb{N}$ est une partie majorée de $\mathbb{R}$; $\mathbb{N}$ étant non vide, l'axiome **BS** nous assure alors l'existence d'un réel α tel que $\alpha = \sup \mathbb{N}$.
Quel que soit $\varepsilon > 0$ il existe donc p de $\mathbb{N}$ tel que

$$\alpha - \varepsilon < p.$$

Prenons $\varepsilon = \frac{1}{2}$ on aura $\alpha - \frac{1}{2} < p$ d'où $\alpha + \frac{1}{2} < p + 1$ c'est-à-dire comme $\alpha < \alpha + \frac{1}{2}$ on aurait, si (non P) est vraie

$$\alpha < p + 1;$$

ceci est faux puisque $p + 1 \in \mathbb{N}$ et $\alpha = \sup \mathbb{N}$, donc (non P) est faux et (P) est vrai.

Théorème.

Quel que soit le nombre réel a il existe un entier naturel n tel que

$$a < n.$$

Cette propriété est connue traditionnellement sous le nom de propriété d'ARCHIMÈDE.

REMARQUES

1. On énonce souvent la propriété d'ARCHIMÈDE sous la forme : quel que soit le réel $x > 0$ et quel que soit le réel y il existe un entier naturel n tel que :

   $$y < nx.$$

   Comme $x > 0$ et que $\mathbb{R}$ est un corps cette relation équivaut à $a < n$ en posant $a = yx^{-1}$.

2. Nous avons vu au chapitre 1 que la propriété d'Archimède est vraie dans $\mathbb{N}$. Dans $\mathbb{Z}$ on a également : quel que soit $x \in \mathbb{Z}_+^* = \mathbb{N}^*$ et quel que soit y de $\mathbb{Z}$ il existe n de $\mathbb{N}$ tel que :

   $$y < nx;$$

   en effet cette propriété est évidente pour $y \leqslant 0$ et si $0 < y$ nous avons la propriété d'ARCHIMÈDE dans $\mathbb{N}$.
   Il en résulte que cette propriété est encore vraie dans $\mathbb{Q}$ car si p, q, r, s, n sont des entiers avec $p > 0$, $q > 0$, $s > 0$, $n > 0$ on a :

   $$\left(\frac{s}{r} < \frac{p}{q}\, n\right) \Longleftrightarrow (sq < (pr)\, n).$$

3. L'axiome **BS** joint aux autres propriétés fondamentales de $(\mathbb{R}, +, \times, \leqslant)$ nous a permis de démontrer dans $\mathbb{R}$ la propriété d'ARCHIMÈDE; on pourrait se demander si cette propriété, jointe aux autres propriétés de $\mathbb{R}$ permet de démontrer la propriété **BS.**
Il n'en est rien car, si c'était possible, $\mathbb{Q}$, étant comme $\mathbb{R}$ un corps totalement ordonné et possédant la propriété d'ARCHIMÈDE (cf. remarque 2 ci-dessus), on pourrait démontrer de la même façon que $\mathbb{Q}$ possède **BS,** ce qui est faux.

b) Application 1. Partie entière d'un nombre réel.

D'après le théorème précédent quel que soit x de $\mathbb{R}$ l'ensemble E des *entiers relatifs strictement supérieurs* à x est non vide, en effet E contient $p \in \mathbb{N} \subset \mathbb{Z}$ tel que $x < p$. L'ensemble E est donc une *partie minorée non vide* de $\mathbb{Z}$; E a donc un *plus petit élément unique* (cf. § 2.2 d), nous pouvons désigner ce plus petit élément de E par $n + 1$.
L'entier n est donc inférieur à x puisque $n + 1$ est le plus petit entier relatif strictement supérieur à x. Concluons :

Théorème et définition.

Quel que soit le nombre réel x; il existe un entier relatif unique n tel que

$$n \leqslant x < n + 1.$$

Cet entier n est appelé partie entière du réel x ; on le note $[x]$.

Si $n < x$, posons $p = n$ on a $p < x < p + 1$,
si $n = x$, posons $p = n - 1$ on a $x = p + 1$;
dans les deux cas on peut énoncer :

Corollaire.

Quel que soit le nombre réel x il existe un entier relatif unique p tel que $p < x \leqslant p + 1$.

c) Application 2. Valeurs approchées à α^{-n} près ($\alpha > 0$) d'un nombre réel.

Choisissons un nombre réel $\alpha > 0$. Pour tout n de $\mathbb{N}$ on a $\alpha^n > 0$ et $\alpha^{-n} > 0$.
Quel que soit le nombre réel x désignons par p_n la partie entière de $\alpha^n x$ on a donc

$$p_n \leqslant \alpha^n x < (p_n + 1)$$

c'est-à-dire

$$p_n \alpha^{-n} \leqslant x < (p_n + 1)\, \alpha^{-n}.$$

Le nombre $p_n \alpha^{-n}$ est appelé **valeur approchée par défaut de x à α^{-n} près.**
— $(p_n + 1)\, \alpha^{-n}$ — **valeur approchée par excès** —
On a pour tout n de $\mathbb{N}$

$$x \in [p_n \alpha^{-n}, (p_n + 1)\, \alpha^{-n}[,$$

et, a fortiori,

$$x \in [p_n \alpha^{-n}, (p_n + 1)\, \alpha^{-n}].$$

On voit que $p_n \alpha^{-n}$ est le *plus grand multiple entier* de α^{-n} *inférieur* à x et que, par conséquent, $(p_n + 1)\, \alpha^{-n}$ est le *plus petit multiple entier* de α^{-n} *strictement supérieur* à x.

Dans la pratique on est amené à prendre $\alpha = \frac{1}{10}$ (numération décimale) ou $\alpha = \frac{1}{2}$ (numération binaire).
D'une manière générale si $0 < \alpha < 1$ nous verrons que les segments $[p_n \alpha^{-n}, (p_n + 1)\, \alpha^{-n}]$ $(n \in \mathbb{N})$ vérifient les conditions du théorème des segments emboîtés et que par conséquent la suite infinie de nombres entiers $p_0, p_1, \ldots, p_n, \ldots$ définit le nombre réel x.

Pour $\alpha = \frac{1}{10}$ les valeurs approchées par défaut et par excès $p_n 10^{-n}$ et $(p_n + 1)\, 10^{-n}$ sont appelées **valeurs approchées décimales d'ordre** n du nombre réel x.

d) Application 3. Densité de $\mathbb{Q}$ dans $\mathbb{R}$.

Soient deux réels *distincts* quelconques a et b; nous désignons par a le plus petit on a donc $a < b$. Nous allons montrer d'abord qu'il existe au moins un rationnel dans $]a, b[$, puis qu'il en existe une infinité.

Le nombre réel $b - a$ est strictement positif; d'après la propriété d'ARCHIMÈDE il existe n de $\mathbb{N}$ tel que

$$\frac{1}{b-a} < n;$$

on a $0 < n$ donc

$$\frac{1}{n} < b - a.$$

L'entier n étant ainsi choisi, considérons le nombre réel nb, d'après le corollaire du sous-paragraphe précédent il existe un entier relatif p unique tel que

$$p < nb \leqslant p + 1,$$

on a donc

$$\frac{p}{n} < b \leqslant \frac{p+1}{n}.$$

Montrons que $a < \frac{p}{n}$; on a

$$\frac{p}{n} - a = \frac{p}{n} + (b - a) - b > \frac{p}{n} + \frac{1}{n} - b = \frac{p+1}{n} - b \geqslant 0$$

donc $0 < \frac{p}{n} - a$; on a par conséquent

$$a < \frac{p}{n} < b.$$

Lemme.

Quels que soient les nombres réels distincts a et b $(a < b)$ il existe au moins un rationnel r appartenant à $]a, b[$.

L'ensemble A des *rationnels strictement compris entre les réels* a et b $(a < b)$ est donc non vide.

Supposons A *fini*; il existe donc un entier naturel $n > 0$ tel que

$$A = \{r_1, r_2, \ldots, r_n\}.$$

Soit r le plus petit des rationnels $r_1, r_2 \ldots, r_n$, les deux nombres a et r sont des nombres réels distincts et il n'existe aucun rationnel dans $]a, r[$ ce qui est contraire au lemme; notre hypothèse, A fini, est donc fausse; concluons :

Théorème et définition.

Quels que soient les nombres réels distincts a et b $(a < b)$ il existe une infinité de rationnels appartenant à $]a, b[$. On exprime cette propriété en disant que $\mathbb{Q}$ est **dense** dans $\mathbb{R}$.

IV. Suites de nombres réels

3. 15 GÉNÉRALITÉS

a) Définitions. Exemples.

Conformément à ce que nous avons dit au § 1, une **suite de nombres réels** est une *application d'une partie* I de $\mathbb{N}$ dans $\mathbb{R}$

$$\begin{aligned} f : \mathrm{I} &\longrightarrow \mathbb{R} \\ n &\longmapsto f(n). \end{aligned}$$

Au lieu de suite de nombres réels, on dit aussi *suite réelle*.
On utilise plutôt la *notation indicielle* en posant $f(n) = u_n$ et on notera la suite $(u_n)_{n \in \mathrm{I}}$; si $\mathrm{I} = \mathbb{N}$ on écrira donc $(u_n)_{n \in \mathbb{N}}$.
On ne confondra pas les notations :

- $(u_n)_{n \in \mathrm{I}}$ **application** f de $\mathrm{I} \subset \mathbb{N}$ dans $\mathbb{R}$
- u_n **nombre réel** qui est la *valeur* $f(n)$ de f pour n.

La suite $(u_n)_{n \in \mathrm{I}}$ est donc définie par l'ensemble des couples (n, u_n) lorsque n décrit I.
On dit que u_n est le **terme d'indice** n de la suite $(u_n)_{n \in \mathrm{I}}$.
L'*ensemble des valeurs* de la suite soit f (I) se notera par exemple, si $\mathrm{I} = \mathbb{N}$, $\{u_0, u_1, \ldots, u_n, \ldots\}$ ou, d'une manière générale, $\{u_n\}_{n \in \mathrm{I}}$ en distinguant bien les parenthèses utilisées pour écrire la suite $(u_n)_{n \in \mathrm{I}}$ et les accolades employées pour désigner l'ensemble des valeurs $\{u_n\}_{n \in \mathrm{I}}$.
Si I est fini on dit que la *suite est finie*; si I est infini on dit que la *suite est infinie* : c'est par exemple le cas où I est $\mathbb{N}$ ou $\mathbb{N}^*$ ou l'ensemble des entiers naturels pairs, impairs, etc.

ATTENTION. Si la suite est finie l'ensemble de ces valeurs est fini. En revanche l'*ensemble des valeurs d'une suite* **infinie** *peut être* **fini**; par exemple la suite définie pour tout n de $\mathbb{N}^*$ par

$$u_n = (-1)^n$$

est une suite *infinie*, son graphe est formé des couples tous distincts

$$(1, -1) \quad (2, 1) \quad (3, -1) \quad \ldots \quad (2p, 1) \quad (2p + 1, -1) \quad \ldots$$

et cependant cette suite ne prend que *deux* valeurs 1 ou -1 ; son ensemble de valeurs est $\{-1, 1\}$.

EXEMPLES

1. $(n^2 - 7n + 49)_{1 \leqslant n \leqslant 6}$ est une suite finie.
2. $(\sin \alpha n)_{n \in \mathbb{N}}$ où α est un nombre réel donné est une suite infinie.
3. $\left(\frac{1}{n}\right)_{n \in \mathbb{N}^*}$ est une suite infinie.
4. $\left((-1)^n + \frac{1}{n}\right)_{n \in \mathbb{N}}$ est une suite infinie.

Par souci de simplification nous noterons désormais (u_n) *toute suite indexée par* $\mathbb{N}$ (*c'est-à-dire telle que* $\mathrm{I} = \mathbb{N}$).

b) Propriétés éventuelles d'une suite de nombres réels.

Une suite de nombres réels étant une application de $I \subset \mathbb{N}$ dans $\mathbb{R}$ c'est-à-dire une *fonction numérique*, nous pouvons *appliquer aux suites certaines des définitions que nous avons données pour les fonctions numériques de variable réelle.*

La suite $(u_n)_{n \in I}$ est **majorée** (resp. **minorée**) s'il existe un réel A tel que pour tout n de I on ait $u_n \leqslant A$ (resp. $A \leqslant u_n$).

Une suite majorée et minorée est dite **bornée.** Par exemple la suite $(3n - 4)$ n'est ni majorée ni minorée, la suite $(\sin n)$ est bornée car pour tout n de $\mathbb{N}$ on a $|\sin n| \leqslant 1$.

La suite $(u_n)_{n \in I}$ est **croissante** si, quels que soient n et n' de I, on a

$$(n \leqslant n') \Longrightarrow (u_n \leqslant u_{n'}),$$

strictement croissante si, quels que soient n et n' de I

$$(n < n') \Longrightarrow (u_n < u_{n'}).$$

Vous définirez sans peine une suite **décroissante** et une suite **strictement décroissante.**

L'ensemble des suites croissantes et des suites décroissantes est appelé ensemble des suites **monotones.**

L'ensemble des suites strictement croissantes et des suites strictement décroissantes est appelé ensemble des suites **strictement monotones.**

Dans les définitions suivantes le vocabulaire est particulier aux suites.

Étant donné $J \subset I \subset \mathbb{N}$ on dit que la suite $(u_n)_{n \in J}$ est **extraite** de la suite $(u_n)_{n \in I}$.

Nous voyons que la suite extraite de $(u_n)_{n \in I}$ définie par

$$\begin{array}{ccc} J & \longrightarrow & \mathbb{R} \\ n & \longmapsto & u_n \end{array}$$

est la **restriction** à J de la suite $(u_n)_{n \in I}$

$$\begin{array}{ccc} I & \longrightarrow & \mathbb{R} \\ n & \longmapsto & u_n \end{array}$$

Par exemple si nous désignons par P^* l'ensemble des entiers naturels pairs non nuls et I l'ensemble des entiers naturels impairs les deux suites

$$\left((-1)^n + \frac{1}{n}\right)_{n \in P^*} \qquad \left(u_n = 1 + \frac{1}{n}\right)$$

$$\left((-1)^n + \frac{1}{n}\right)_{n \in I} \qquad \left(u_n = -1 + \frac{1}{n}\right)$$

sont deux suites extraites de la suite de l'exemple 4 ci-dessus.

On dit qu'une *suite infinie* est **stationnaire** s'il existe un entier p tel que quel que soit n de I

$$(n \geqslant p) \Longrightarrow (u_n = u_p).$$

Par exemple si $I = \mathbb{N}$ cela signifie que la suite (u_n) est *constante* sur $[p, +\infty[$.

c) Opérations algébriques sur les suites.

Là encore nous ne faisons qu'appliquer aux suites le vocabulaire relatif aux fonctions numériques.

Soit $(u_n)_{n \in I}$, $(v_n)_{n \in I}$ deux suites indexées par le même ensemble I partie de $\mathbb{N}$, c'est-à-dire deux éléments de $\mathcal{F}(I, \mathbb{R})$ et λ un nombre réel quelconque on a

(1) $\quad (u_n)_{n \in I} + (v_n)_{n \in I} = (u_n + v_n)_{n \in I}$

(2) $\quad (u_n)_{n \in I} (v_n)_{n \in I} = (u_n v_n)_{n \in}$

(3) $\quad \lambda (u_n)_{n \in I} = (\lambda u_n)_{n \in I}$

On définit ainsi la **somme** (1), le **produit** (2) des deux suites $(u_n)_{n\in I}$ et $(v_n)_{n\in I}$ et le **produit par le réel** α de la suite $(u_n)_{n\in I}$.

EXERCICES

On pose $\mathcal{S} = \mathcal{F}(I, \mathbb{R})$. $I \subset \mathbb{N}$

1. Démontrer que $(\mathcal{S}, +)$ est un groupe commutatif. En particulier la suite $(-u_n)$ se note $-(u_n)$.
2. Démontrer que $(\mathcal{S}, +, \times)$ est un anneau commutatif unitaire.
3. Démontrer que $(\mathcal{S}, +, .)$ — où le point . désigne la multiplication par un réel — est un espace vectoriel sur $\mathbb{R}$.

Si pour tout n de I on a $u_n \neq 0$ la suite $\left(\frac{1}{u_n}\right)_{n\in I}$ est l'**inverse** de la suite $(u_n)_{n\in I}$.

Dans la pratique on étendra un peu cette définition; considérons $I' \subset I$ tel que pour tout n de I' on ait $u_n \neq 0$, on dira que la suite $\left(\frac{1}{u_n}\right)_{n\in I'}$ est l'inverse de la suite $(u_n)_{n\in I}$.

Par exemple la suite $\left(\frac{1}{n}\right)_{n\in \mathbb{N}^*}$ est l'inverse de la suite $(n)_{n\in\mathbb{N}}$; c'est un abus de langage.

Avec deux suites $(u_n)_{n\in I}$ et $(v_n)_{n\in I}$ on pourra définir la suite $\left(\frac{u_n}{v_n}\right)_{n\in I'}$ (pour tout n de I' on suppose $v_n \neq 0$).

Enfin on dira que la suite $(|u_n|)_{n\in I}$ est la *valeur absolue* de la suite $(u_n)_{n\in I}$.

3. 16 SUITES ARITHMÉTIQUES ET SUITES GÉOMÉTRIQUES RÉELLES

a) Suites arithmétiques de nombres réels.

Soit une suite réelle (u_n) telle que pour tout entier naturel non nul on ait

(1) $$u_n = \frac{u_{n-1} + u_{n+1}}{2}$$

c'est-à-dire que chaque terme, à partir de u_1, est égal à la *moyenne arithmétique* des deux termes qui l'encadrent; l'égalité (1) est équivalente à

(2) $$u_n - u_{n-1} = u_{n+1} - u_n.$$

Donc il existe un réel r tel que pour tout n on ait

(3) $$u_{n+1} - u_n = r.$$

Définition.

On appelle **suite arithmétique** de nombres réels toute suite réelle (u_n) possédant la propriété suivante : il existe un réel r tel que, pour tout entier naturel n,

$$u_{n+1} - u_n = r.$$

Le nombre réel r est appelé **raison** de la suite arithmétique considérée.

Si on pose $u_0 = a$ on voit que $u_1 = a + r$ et on montrera facilement par récurrence que pour tout n de $\mathbb{N}$ on a

(4) $$\boxed{u_n = a + rn}.$$

Réciproquement on voit que toute suite réelle (u_n) définie pour tout n par $u_n = \alpha + \beta n$ est la suite arithmétique de raison β telle que $u_0 = \alpha$.

REMARQUE

1. La suite extraite d'une suite arithmétique relative à $I = [0, n]$ est appelée *progression arithmétique*; traditionnellement la suite que nous appelons suite arithmétique est appelée « progression arithmétique illimitée ». Il arrive aussi de considérer des « progressions arithmétiques illimitées dans les deux sens »; ce sont les applications

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{R} \\ n & \longmapsto & a + rn \end{array}$$

dont les valeurs peuvent s'écrire :

$$\ldots\ a - nr,\ \ldots\ a - r,\ a,\ a + r,\ \ldots.,\ a + nr,\ \ldots..$$

On voit que si $r = 0$ la suite (u_n) est constante, qu'elle est strictement croissante si $r > 0$ et strictement décroissante si $r < 0$.

Calcul de $S_n = u_0 + u_1 + \ldots + u_n$.

Soit h un entier tel que $0 \leqslant h \leqslant n$ nous avons

$$u_h + u_{n-h} = a + hr + a + (n - h)\,r = a + a + nr = u_0 + u_n;$$

il en résulte que si l'on écrit

$$\begin{aligned} S_n &= u_0 + u_1 + \ldots + u_h + \ldots + u_{n-1} + u_n. \\ S_n &= u_n + u_{n-1} + \ldots + u_{n-h} + \ldots + u_1 + u_0 \end{aligned}$$

on obtient, en ajoutant ces deux égalités par colonnes

$$2\,S_n = (n + 1)\,(u_0 + u_n)$$

car il y a, de 0 à n, $n + 1$ indices; d'où

(5) $$\boxed{S_n = (n + 1)\frac{u_0 + u_n}{2}}.$$

ATTENTION : Dans S_n il y a $n + 1$ termes. D'une manière générale si on prend n *termes consécutifs* d'une suite arithmétique le premier étant a le dernier l leur somme est

$$S = n\frac{a + l}{2}.$$

Par exemple on a $(a = 1, l = n)$

$$1 + 2 + \ldots + n = \frac{n\,(n + 1)}{2}.$$

EXERCICE

1. Étant donnés une suite arithmétique (u_n) de raison r et un entier $k \geqslant 2$, trouver une suite arithmétique (v_n) telle que pour tout n :

$$v_{kn} = u_n.$$

On trouvera que la raison de (v_n) est $r' = \frac{r}{k}$; le schéma :

$$\begin{array}{ccccccc} u_n & & & & & & u_{n+1} \\ v_{kn} & v_{kn+1} & \cdots & v_{kn+k-1} & & v_{kn+k} & \end{array}$$

explique le nom donné à cette opération : *insertion de* k − 1 *moyens arithmétique entre deux termes consécutifs d'une suite arithmétique.*

b) Suites géométriques de nombres réels.

Soit une suite (u_n) de nombres réels telle que pour tout entier naturel non nul on ait

(1′) $$(u_n)^2 = u_{n-1}\, u_{n+1},$$

c'est-à-dire que chaque terme à partir de u_1 est *moyenne géométrique* des deux termes qui l'encadrent.

Si tous les termes de (u_n) sont *non nuls* l'égalité (1′) est équivalente à

(2′) $$\frac{u_n}{u_{n-1}} = \frac{u_{n+1}}{u_n}.$$

Donc il existe un nombre réel *non nul* q tel que pour tout n on ait

(3′) $$u_{n+1} = qu_n.$$

L'égalité (3′) ayant un sens même pour $u_n = 0$ nous poserons la définition suivante :

Définition.

On appelle **suite géométrique** de nombres réels toute suite réelle (u_n) possédant la propriété suivante : il existe un nombre réel q tel que, pour tout entier naturel n,

$$u_{n+1} = qu_n.$$

Le nombre réel q est appelé **raison** de la suite géométrique considérée.

Si $q = 0$ tous les termes à partir de u_1 sont *nuls*. Nous supposerons dans la suite que $q \neq 0$.

Si on pose $u_0 = a$ on voit que $u_1 = aq$ et on montrera facilement par récurrence que pour tout n de $\mathbb{N}$ on a

(4′) $$\boxed{u_n = aq^n}.$$

Réciproquement on voit que toute suite réelle (u_n) définie pour tout n par $u_n = \alpha\beta^n$ ($\beta \neq 0$) est la suite géométrique de raison β telle que $u_0 = \alpha$.

REMARQUE

2. La suite extraite d'une suite géométrique relative à $I = [0, n]$ est appelée *progression géométrique*; traditionnellement la suite que nous appelons suite géométrique est appelée « progression géométrique illimitée ». Il arrive également de considérer des « progressions géométriques illimitées dans les deux sens »; ce sont les applications :

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{R} \\ a & \longmapsto & aq^n \end{array}$$

dont les valeurs peuvent s'écrire :

$$\ldots\ aq^{-n},\ \ldots,\ aq^{-1},\ a,\ aq,\ \ldots,\ aq^n,\ \ldots$$

Soit la suite géométrique (aq^n) où $q \neq 0$. Si $u_0 = a = 0$ alors tous les nombres u_n sont nuls; nous supposerons dans la suite que $u_0 = a \neq 0$, il en résulte que $u_n \neq 0$ pour tout n.

Si $0 < q$ tous les nombres réels u_n ont le même signe celui de $u_0 = a$. On voit que la suite (aq^n) est constante pour $q = 1$. Si $a > 0$ et $q > 1$ la suite est strictement croissante; si $a > 0$ et $0 < q < 1$ la suite est strictement décroissante; les résultats sont inversés si $a < 0$.

Si $q < 0$ tous les réels u_{2n} ont le signe de u_0 et les réels u_{2n+1} ont le signe opposé à celui de u_0; on dit qu'une telle suite réelle est *alternée*.

Calcul de $S_n = u_0 + u_1 + \ldots + u_n$.

Nous avons

$$S_n = u_0 + \ldots + u_n = a + aq + \ldots + aq^n = a(1 + q + \ldots + q^n).$$

Une identité remarquable obtenue au § 3.10 nous permet d'écrire

$$(1 - q)(1 + q + \ldots + q^n) = 1 - q^{n+1}.$$

Donc si q **est distinct de 1**

(5') $$\boxed{S_n = a\,\frac{1 - q^{n+1}}{1 - q}}.$$

Si $q = 1$ on a $S_n = (n + 1)\,a$.

ATTENTION. Le S_n que nous avons écrit est relatif aux $n + 1$ premiers termes de la suite (aq^n).

EXERCICE

2. Étant donnés une suite géométrique (u_n) de raison q et un entier $k \geqslant 2$, trouver une suite géométrique (v_n) telle que, pour tout n, on ait :

$$v_{kn} = u_n.$$

On trouvera que, si (v_n) existe, sa raison q' est telle que :

$$q'^k = q.$$

Si k est impair il y a toujours une solution unique.

Si k est pair il n'y a pas de solution pour $q < 0$ et deux solutions $q^{\frac{1}{k}}$ et $-q^{\frac{1}{k}}$ si $0 < q$.

Le schéma :

$$\begin{array}{ccccccc} u_n & & & & & & u_n \\ v_{kn} & v_{kn+1} & \cdots & & v_{kn+k-1} & & v_{kn+k} \end{array}$$

explique le nom donné à cette opération : « insertion de $k - 1$ moyens arithmétiques entre deux termes consécutifs d'une suite géométrique ».

3. 17 ÉTUDE D'UNE SUITE INFINIE RÉELLE (u_n) LORSQUE n TEND VERS $+\infty$.

Soit f une fonction numérique définie dans $[a, +\infty[$; nous avons étudié en Première les situations concernant f et nous permettant d'écrire

$$\lim_{x \to +\infty} f(x) = l \quad , \quad \lim_{x \to +\infty} f(x) = +\infty \quad , \quad \lim_{x \to +\infty} f(x) = -\infty.$$

Nous allons transposer ces définitions aux suites réelles.

Pour simplifier nous supposerons (u_n) définie pour tout n de $\mathbb{N}$, vous n'aurez aucun mal à étendre ces définitions au cas où (u_n) serait définie seulement pour $n \geqslant k$.

a) Suites convergentes.

Définition 1.

On dit que la suite infinie réelle (u_n) a pour **limite** l lorsque n tend vers $+\infty$ si et seulement si on a

$$(\forall\, \varepsilon \in \mathbb{R}_+^*)\ (\exists\, p \in \mathbb{N})\ (\forall\, n \in]p, +\infty[) \qquad |u_n - l| < \varepsilon.$$

On dit alors que la suite (u_n) est **convergente.**

On écrira $\lim\limits_{n \to +\infty} u_n = l$ ou plus simplement

$$\lim u_n = l.$$

Pour prouver $\lim u_n = l$, on se *donnera* arbitrairement $\varepsilon > 0$; il suffira alors de *trouver* p de $\mathbb{N}$ tel que, pour tout n de $\mathbb{N}$,

$$(n > p) \Longrightarrow (|u_n - l| < \varepsilon).$$

REMARQUES

1. On verra sans peine que l'on peut remplacer $]p, +\infty[$ par $[p, +\infty[$ ou $|u_n - l| < \varepsilon$ par $|u_n - l| \leqslant \varepsilon$.
2. On n'oubliera pas que l'écriture condensée $|u_n - l| < \varepsilon$ signifie :
$$l - \varepsilon < u_n < l + \varepsilon,$$
double inégalité beaucoup plus facile à manier dans les calculs que l'inégalité $|u_n - l| < \varepsilon$.
3. On voit immédiatement que $\lim u_n = 0$ signifie $\lim |u_n| = 0$ et d'une manière plus générale :
$$(\lim u_n = l) \Longleftrightarrow (\lim |u_n - l| = 0).$$

EXEMPLES

1. Soit la suite $\left(\dfrac{2n+3}{n-1}\right)$ définie pour $n \geqslant 2$. On a
$$\left|\frac{2n+3}{n-1} - 2\right| = \left|\frac{5}{n-1}\right|.$$
Donnons-nous arbitrairement $\varepsilon > 0$ on aura $\dfrac{5}{n-1} < \varepsilon$ si on a $n > \dfrac{5}{\varepsilon} + 1$; choisissons un entier $p \geqslant \sup\left(2, \dfrac{5}{\varepsilon} + 1\right)$; quel que soit n on aura
$$(n > p) \Longrightarrow (|u_n - 2| < \varepsilon).$$
Donc $\lim\limits_{n \to +\infty} \dfrac{2n+3}{n-1} = 2$.
2. Soit la suite $(\sqrt{n+1} - \sqrt{n})$ définie pour tout $n > 0$; on a
$$u_n = \sqrt{n+1} - \sqrt{n} = \frac{1}{\sqrt{n+1} + \sqrt{n}} < \frac{1}{2\sqrt{n}}.$$
Donc pour tout $\varepsilon > 0$ on aura $|u_n| < \varepsilon$ si on a $\dfrac{2}{\sqrt{n}} < \varepsilon$ c'est-à-dire $n > \dfrac{4}{\varepsilon^2}$; choisissons un entier $p \geqslant \dfrac{4}{\varepsilon^2}$; pour tout n on aura
$$(n > p) \Longrightarrow |u_n| < 0.$$
Donc $\lim (\sqrt{n+1} - \sqrt{n}) = 0$.
3. Toute suite stationnaire est convergente : s'il existe p tel que $n \geqslant p$ entraîne $u_n = u_p$, on aura $\lim u_n = u_p$.

EXERCICE

1. Montrer que si (u_n) est convergente on a
$$\lim |(u_n)| = |\lim u_n|$$
(On utilisera la relation $\big||u_n| - |l|\big| \leqslant |u_n - l|$.)

Exemple 4. Suites adjacentes.

Considérons une suite d'intervalles fermés $[a_n, b_n]$ vérifiant les conditions du *théorème des intervalles emboîtés* (cf. § 3.13). Les deux suites (a_n) et (b_n) vérifient donc les propriétés suivantes :

1. Pour tout n de $\mathbb{N}$

$$a_n \leqslant a_{n+1} \leqslant b_{n+1} \leqslant b_n.$$

2. Quel que soit le réel $\varepsilon > 0$ il existe un entier p tel que

$$b_p - a_p < \varepsilon.$$

Nous savons alors qu'il existe un *réel unique* appartenant à *tous* les segments $[a_n, b_n]$; si on le désigne par l on a

$$l = \sup_{n \in \mathbb{N}} a_n = \inf_{n \in \mathbb{N}} b_n.$$

Avec les notations ci-dessus on voit que pour tout $n > p$ on aura

$$a_p \leqslant a_n \leqslant l \leqslant b_n \leqslant b_p;$$

et, comme $b_p - a_p < \varepsilon$, on aura pour tout n

$$(n > p) \Longrightarrow (|a_n - l| < \varepsilon \quad \text{et} \quad |b_n - l| < \varepsilon).$$

Donc
$$\lim_{n \to +\infty} a_n = \lim_{n \to +\infty} b_n = l.$$

On voit même que (a_n) atteint sa limite l par *valeurs inférieures* et (b_n) par *valeurs supérieures*; on écrira

$$\lim_{n \to +\infty} a_n = l - 0 \quad , \quad \lim_{n \to +\infty} b_n = l + 0.$$

La situation considérée pour les suites (a_n) et (b_n) peut se formuler ainsi :

1'. *La suite (a_n) est croissante; la suite (b_n) est décroissante et pour tout n de $\mathbb{N}$ on a* $a_n \leqslant b_n$.

2'. $\operatorname{Lim}_{n \to +\infty} (b_n - a_n) = 0.$

Tout couple de suites réelles (a_n) et (b_n) vérifiant ces deux conditions est appelé couple de **suites adjacentes.**

Deux suites adjacentes (a_n) et (b_n) sont *convergentes* et ont pour limite commune le *réel unique* appartenant à tous les intervalles $[a_n, b_n]$.

Dans l'étude des calculs approchés (cf. § 3.21 a) nous rencontrerons un exemple remarquable de suites adjacentes : les suites des valeurs approchées par défaut et par excès à 10^{-n} près d'un réel.

b) Suites réelles (u_n) tendant vers $+\infty$ (resp. $-\infty$) lorsque n tend vers $+\infty$.

Définition 2.

On dit que la suite infinie réelle (u_n) tend vers $+\infty$ lorsque n tend vers $+\infty$ si et seulement si on a

$$(\forall A \in \mathbb{R}_+^*) \quad (\exists p \in \mathbb{N}) \quad (\forall n \in]p, +\infty[) \qquad u_n > A.$$

On écrit dans ce cas $\lim_{n \to +\infty} u_n = +\infty$ ou plus simplement

$$\lim u_n = +\infty.$$

Pour prouver que $\lim u_n = +\infty$, on se donnera arbitrairement $A > 0$, il suffira alors de trouver p de $\mathbb{N}$ tel que, pour tout n de $\mathbb{N}$

$$(n > p) \Longrightarrow (u_n > A).$$

De même la notation $\lim u_n = -\infty$ qui se lit « *la suite u_n tend vers $-\infty$ lorsque n tend vers $+\infty$* » signifie

$$(\forall A \in \mathbb{R}_+^*) \quad (\exists p \in \mathbb{N}) \quad (\forall n \in]p, +\infty[) \qquad u_n < -A.$$

REMARQUES

4. On peut dans ces définitions remplacer $]p, +\infty[$ par $[p, +\infty[$ ou $u_n > A$ (resp. $u_n < A$) par $u_n \geqslant A$ (resp. $u_n \leqslant -A$).

5. Si $\lim u_n = +\infty$ ou bien $\lim u_n = -\infty$, on aura $\lim |u_n| = +\infty$. Réciproquement si $\lim |u_n| = +\infty$ et *si à partir d'un certain rang k le réel u_n garde un signe constant* on aura $\lim u_n = +\infty$ ou bien $\lim u_n = -\infty$. En revanche si le réel u_n ne garde pas un signe constant à partir d'un certain rang, on peut avoir $\lim |u_n| = +\infty$ sans avoir $\lim u_n = +\infty$ ou bien $\lim u_n = -\infty$, c'est ce qui se passe pour la suite alternée $((-1)^n n)$.

EXEMPLE

5. Soit une *suite arithmétique* $(a + rn)$ où $r \neq 0$; on voit immédiatement que

si $r > 0$ $\quad \lim (a + rn) = +\infty$
si $r < 0$ $\quad \lim (a + rn) = -\infty$

Démontrons par exemple la deuxième proposition. Soit un réel $A > 0$ arbitraire. On aura $a + rn < -A$ si on a $n > \dfrac{-A - a}{r}$ (car $r < 0$); choisissons un entier $p \geqslant \sup\left(-\dfrac{A + a}{r}, 0\right)$; pour tout n on aura

$$(n > p) \Longrightarrow (u_n < -A)$$

donc $\lim u_n = -\infty$.

ATTENTION. Lorsque $\lim u_n = +\infty$ ou $\lim u_n = -\infty$ on dit quelquefois que (u_n) admet une *limite infinie;* c'est un *abus de langage*, de même que $\lim u_n = +\infty$ (ou $\lim u_n = -\infty$) est un *abus de notation* commode.

Lorsque nous dirons (u_n) a une limite, il s'agira toujours d'une limite au sens de la définition 1, c'est-à-dire une limite *l* élément de $\mathbb{R}$.

c) Étude d'autres situations.

Comme le montre l'exemple et les exercices suivants, les deux cas étudiés, suite convergente et suite tendant vers $+\infty$ (resp. $-\infty$) lorsque n tend vers $+\infty$, n'épuisent pas tous les cas possibles.

Exemple 6. Soit la suite (u_n) définie pour tout n de $\mathbb{N}$ par

$$u_n = n \text{ pour } n \text{ pair},$$
$$u_n = \frac{1}{n} \text{ pour } n \text{ impair}.$$

Les termes de (u_n) s'écrivent

$$0 \quad 1 \quad 2 \quad \frac{1}{3} \quad 4 \quad \frac{1}{5} \quad 6 \quad \frac{1}{6} \quad \ldots \; 2k \quad \frac{1}{2k+1} \quad 2k+2 \quad \ldots$$

On voit immédiatement que (u_n) ne satisfait ni à la définition (1) ni à la définition (2).

EXERCICES

Étudier les suites suivantes lorsque n tend vers $+\infty$.

2. $(\forall n \in \mathbb{N}) \quad u_n = a + (-1)^n b \quad (a \in \mathbb{R}, b \in \mathbb{R}^*)$,
3. $(\forall n \in \mathbb{N}^*) \quad u_n = \frac{1}{n} + (-1)^n$,
4. $(\forall n \in \mathbb{N}^*) \quad u_n = (-1)^n n^{(-1)^n}$,
5. $(\forall n \in \mathbb{N}) \quad u_n = \sin \frac{2\pi}{5} n$.

d) Étude de la suite (a^n) $(a \in \mathbb{R}^*)$.

Nous commencerons par démontrer un lemme.

Lemme.

si $a > 1$ alors $\lim_{n \to +\infty} a^n = +\infty$.

Posons $a = 1 + b$, alors $b > 0$. La formule du binôme nous permet d'écrire

$$a^n = (1+b)^n = 1 + nb + \frac{n(n-1)}{2} b^2 + \ldots + b^n.$$

Comme $b > 0$, tous les termes du dernier membre de ces égalités sont strictement positifs donc

$$a^n > nb.$$

Soit A un réel strictement positif arbitraire; pour avoir $a^n > A$ il suffit donc d'avoir $nb > A$, c'est-à-dire $n > \frac{A}{b}$; choisissons un entier $p \geqslant \frac{A}{b}$; pour tout n de $\mathbb{N}$ nous aurons

$$(n > p) \Longrightarrow (a^n > A).$$

Le lemme est donc démontré.

Il résulte du lemme que si $|a| > 1$ on a

$$\lim_{n \to +\infty} |a^n| = +\infty.$$

Si $a < -1$ nous avons une suite alternée; lorsque n tend vers $+\infty$ elle ne tend ni vers $+\infty$, ni vers $-\infty$.

Supposons maintenant $|a| < 1$. Posons $a = \frac{1}{a'}$, nous avons

$$a^n = \frac{1}{a'^n} \quad \text{avec} \quad |a'| > 1.$$

On voit que, dans ce cas, $\lim_{n \to +\infty} a^n = 0$; en effet soit un réel $\varepsilon > 0$ arbitraire on aura $|a^n| < \varepsilon$ si et seulement si $|a'^n| > \frac{1}{\varepsilon}$. Comme $\lim |a'^n| = +\infty$ il existe un entier p tel que pour tout n on ait

$$(n > p) \Longrightarrow \left(|a'^n| > \frac{1}{\varepsilon}\right) \Longleftrightarrow (|a^n| < \varepsilon).$$

On a donc, dans ce cas, $\lim a^n = 0$.

Enfin si $|a| = 1$, pour $a = +1$, a^n est une suite constante et, pour $a = -1$, c'est la suite alternée $(-1)^n$ qui prend les valeurs 1 ou -1.
Résumons cette étude :

Théorème.

Pour tout réel **non nul** a

si $|a| < 1$ alors $\lim\limits_{n\to+\infty} a^n = 0$,
si $|a| > 1$ alors $\lim\limits_{n\to+\infty} |a^n| = +\infty$,
si $a = 1$ la suite (a^n) est constante et prend la valeur 1,
si $a = -1$ la suite (a^n) est alternée et prend les valeurs 1 ou -1.

Remarquons que si $a = 0$ et pour tout n de $\mathbb{N}^*$, on a aussi $a^n = 0$.
On peut également dire que la suite (a^n) est convergente si et seulement si $-1 < a \leqslant 1$; mais, pour $-1 < a < 1$, la limite est *zéro* et, pour $a = 1$, la limite est *un*.

Les deux paragraphes suivants sont des compléments; la plupart des sujets traités sont des adaptations au langage des suites des situations relatives aux fonctions numériques définies dans $]a, +\infty[$, situations que vous avez rencontrées en Première ou que vous rencontrerez dans le tome 2 de ce cours.

3. 18 COMPLÉMENT 1. PROPRIÉTÉS DES SUITES CONVERGENTES

Soit (u_n) une suite infinie réelle convergente; d'après la définition 1 il existe $l \in \mathbb{R}$ tel que

$$(\forall \varepsilon \in \mathbb{R}_+^*) \quad (\exists p \in \mathbb{N}) \quad (\forall p \in]p, +\infty[) \qquad |u_n - l| < \varepsilon.$$

a) Propriété 1. Unicité de la limite.

Supposons $\lim u_n = l$ et $\lim u_n = l'$. Quel que soit $\varepsilon > 0$ il existe p et p' de $\mathbb{N}$ tels que pour tout n de $\mathbb{N}$

$$(n > p) \Longrightarrow (|u_n - l| < \varepsilon),$$
$$(n > p') \Longrightarrow (|u_n - l'| < \varepsilon).$$

Posons $q = \sup(p, p')$; pour tout $n > q$ on aura à la fois les deux inégalités $|u_n - l| < \varepsilon$ et $|u_n - l'| < \varepsilon$ d'où

$$|l - l'| = |l - u_n + u_n - l'| = |(l - u_n) + (u_n - l')|$$
$$\leqslant |l - u_n| + |u_n - l'| = 2\varepsilon.$$

Il en résulte que $l = l'$ car si $l \neq l'$, il serait impossible que $|l - l'|$ nombre strictement positif soit inférieur à 2ε quel que soit $\varepsilon > 0$: en prenant $0 < \varepsilon < \dfrac{|l - l'|}{2}$ on aurait une impossibilité.

Si une suite infinie réelle a une limite, cette limite est unique.

b) Propriété 2. Toute suite convergente est bornée.

Avec les notations rappelées ci-dessus on a, pour tout $n > p$,

$$l - \varepsilon < u_n < l + \varepsilon.$$

Donc si on pose

$$a = \inf(u_0, u_1, \ldots, u_p, l - \varepsilon)$$
$$b = \sup(u_0, u_1, \ldots, u_p, l + \varepsilon)$$

on aura $a < u_n < b$ pour tout n de $\mathbb{N}$; concluons :

> Toute suite infinie réelle convergente est bornée.

Le contre-exemple fourni par la suite (u_n) définie pour tout n par $u_n = (-1)^n$ montre que la réciproque de cette propriété est fausse, (u_n) est bornée, elle n'est pas convergente.

c) Propriété 3. Suite convergeant vers un réel non nul.

Supposons $\lim u_n = l \neq 0$. Prenons $\varepsilon = \frac{|l|}{2}$, il existe k de $\mathbb{N}$ tel que pour tout n de $\mathbb{N}$

$$(n > k) \Longrightarrow \left(l - \frac{|l|}{2} < u_n < l + \frac{|l|}{2}\right);$$

les deux nombres réels $l - \frac{|l|}{2}$ et $l + \frac{|l|}{2}$ sont *non nuls* et ont le *même signe*, celui de l.

Concluons :

> Si $\lim u_n = l \neq 0$ il existe k de $\mathbb{N}$ tel que pour tout $n > k$ on ait
> $$u_n l > 0.$$

Donc si $l \neq 0$ pour $n > k$ on pourra considérer la suite $\left(\frac{1}{u_n}\right)$.

d) Propriété 4. Limites et ordre.

Soient deux suites convergentes (a_n) et (b_n) de limites respectives a et b. Supposons que pour tout n de $\mathbb{N}$ on ait

$$a_n \leqslant b_n.$$

Nous allons montrer que $a \leqslant b$.

Supposons en effet $b < a$ et prenons $\varepsilon = \frac{a-b}{4} > 0$; il existe p et q de $\mathbb{N}$ tels que pour tout n de $\mathbb{N}$ on ait

$$(n > p) \Longrightarrow (a - \varepsilon < a_n < a + \varepsilon),$$
$$(n > q) \Longrightarrow (b - \varepsilon < b_n < b + \varepsilon).$$

Or $a - \varepsilon - (b + \varepsilon) = a - b - 2\varepsilon = a - b - \frac{a-b}{2} = \frac{a-b}{2} > 0$; donc pour tout $n > r = \sup(p, q)$ on aura

$$b_n < b + \varepsilon < a - \varepsilon < a_n,$$

ce qui est contraire à l'hypothèse $a_n \leqslant b_n$ pour tout n; donc $b < a$ étant faux, on a $a \leqslant b$. Concluons :

> Pour tout couple de suites convergentes (a_n) et (b_n) on a
> $$[(\forall n \in \mathbb{N})\ a_n \leqslant b_n] \Longrightarrow (\lim a_n \leqslant \lim b_n).$$

REMARQUE

1. On voit sans peine que la proposition précédente est vraie si on a seulement $a_n \leqslant b_n$ pour $n \geqslant k$ k étant un entier déterminé; il suffira dans la démonstration précédente de poser $r = \sup(p, q, k)$.

EXERCICE

1. On considère les deux suites définies pour tout n de $\mathbb{N}^*$ par

$$a_n = 1 - \frac{1}{n} \quad \text{et} \quad b_n = 1 + \frac{1}{n}.$$

Démontrer que $\lim a_n = \lim b_n = 1$.

Le résultat de cet exercice montre que si on a, pour tout n, $a_n < b_n$ on peut seulement conclure $\lim a_n \leqslant \lim b_n$. On traduit ce fait en disant qu'il y a *affaiblissement des inégalités par passage à la limite.*

e) **Propriété 5. Suite croissante et majorée (resp. décroissante et minorée).**

Soit (u_n) une suite infinie réelle **croissante** et **majorée.**
Dire que (u_n) est *majorée* signifie que l'ensemble — non vide — V des *valeurs* de la suite (u_n) est majorée. Cet ensemble V a donc une borne supérieure (cf. § 3.11); posons

$$l = \sup V.$$

Quel que soit $\varepsilon > 0$ il existe donc un élément de V soit u_p tel que

$$l - \varepsilon < u_p \leqslant l.$$

D'autre part la suite (u_n) est croissante; donc, pour tout $n > p$ on a

$$l - \varepsilon < u_p \leqslant u_n \leqslant l.$$

Il en résulte que pour tout $\varepsilon > 0$ on a trouvé p de $\mathbb{N}$ tel que quel que soit $n > p$ on ait $|u_n - l| < \varepsilon$ donc $\lim u_n = l$. En fait la double inégalité $l - \varepsilon < u_n \leqslant l$ est plus précise que $l - \varepsilon < u_n < l + \varepsilon$; on traduit ce fait en disant que *la limite l est atteinte par valeurs inférieures* et on écrira

$$\lim u_n = l - 0.$$

On démontrerait de même que toute suite infinie réelle décroissante et minorée est convergente; dans ce cas la limite est atteinte par valeurs supérieures. Concluons :

Toute suite infinie réelle croissante et majorée (resp. décroissante et minorée) est convergente.

EXERCICE

2. Écrire qu'une suite (u_n) est majorée. Puis qu'une suite (u_n) est non majorée (on trouvera

$$(\forall A \in \mathbb{R}_+^*) \quad (\exists p \in \mathbb{N}) \qquad u_p > A)$$

En déduire que toute suite (u_n) *croissante* et *non majorée* tend vers $+\infty$ lorsque n tend vers $+\infty$.

REMARQUE

2. Le résultat de l'exercice précédent est relatif aux suites *non majorées croissantes.* Il ne faudrait pas croire que toute suite non majorée tend vers $+\infty$. L'exemple du § 3.17 *c* de la suite

$$0 \quad 1 \quad 2 \quad \frac{1}{3} \quad 4 \quad \frac{1}{5} \quad 6 \quad \frac{1}{7} \quad \ldots$$

fournit un contre-exemple : cette suite est non majorée et elle ne tend pas vers $+\infty$.

D'ailleurs en écrivant avec des quantificateurs les deux propriétés

- (u_n) est une suite infinie réelle non majorée
- $\lim u_n = +\infty$

on remarquera que ces deux propriétés sont *distinctes* dans le cas général; comme nous l'avons vu à l'exercice 2 elles deviennent identiques si la suite est *croissante*.

3. 19 COMPLÉMENT 2. OPÉRATIONS SUR LES SUITES

Nous distinguerons le cas des suites convergentes et celui des suites tendant vers $+\infty$ (resp. $-\infty$) lorsque n tend vers $+\infty$.

a) Suites convergentes : somme et produit.

Soient deux suites convergentes quelconques (a_n) et (b_n) de limites respectives a et b et un nombre réel quelconque λ; nous allons montrer que les suites (cf. 3.15 c)

$$(a_n) + (b_n) = (a_n + b_n),$$
$$(a_n)\,(b_n) = (a_n b_n),$$
$$\lambda\,(a_n) = (\lambda\, a_n),$$

sont convergentes et calculer leurs limites.

Donnons-nous un réel $\varepsilon > 0$ arbitraire. La relation

$$|\, a_n + b_n - (a + b)\,| = |\,(a_n - a) + (b_n - b)\,| \leqslant |\, a_n - a\,| + |\, b_n - b\,|$$

montre que pour avoir

$$|\, a_n + b_n - (a + b)\,| < \varepsilon$$

il suffit d'avoir

(1) $$|a_n - a| < \frac{\varepsilon}{2},$$

(2) $$|b_n - b| < \frac{\varepsilon}{2}.$$

Or il existe des entiers naturels p et q tels que pour tout n

$$(n \geqslant p) \Longrightarrow |a_n - a| < \frac{\varepsilon}{2},$$

$$(n > q) \Longrightarrow |b_n - b| < \frac{\varepsilon}{2}.$$

En posant $r = \sup(p, q)$ on aura pour tout n

$$(n > r) \Longrightarrow |\, a_n + b_n - (a + b)\,| < \varepsilon.$$

Donc $\lim (a_n + b_n) = \lim a_n + \lim b_n$.

On montrera facilement par récurrence que ce résultat s'étend à k suites convergentes.

Soit la suite $\lambda\,(a_n) = (\lambda\, a_n)$; si $\lambda = 0$ pour tout n on a $\lambda\, a_n = 0$;

donc $\lim (\lambda\, a_n) = 0 = 0 \times \lim a_n$. Supposons $\lambda \neq 0$; Quel que soit n nous avons

$$|\lambda a_n - \lambda l| < \varepsilon \Longleftrightarrow |a_n - l| < \frac{\varepsilon}{|\lambda|};$$

il existe p tel que pour tout $n > p$ on ait $|\, a_n - l\,| < \frac{\varepsilon}{|\lambda|}$; donc $|\,\lambda\, a_n - \lambda\, l\,| < \varepsilon$. Par conséquent $\lim (\lambda\, a_n) = \lambda \lim a_n$.

Pour étudier la suite $(a_n)(b_n) = (a_n b_n)$, posons

$$a_n = a + \alpha_n, \qquad b_n = b + \beta_n;$$

les deux suites (α_n) et (β_n) ont pour limite zéro. Montrons que la suite $(\alpha_n\beta_n)$ a pour limite zéro. En effet quel que soit $\varepsilon > 0$ les relations

$$(1') \qquad |\alpha_n| < \sqrt{\varepsilon},$$

$$(2') \qquad |\beta_n| < \sqrt{\varepsilon}$$

entraînent $|\alpha_n\beta_n| < \varepsilon$. Or il existe des entiers naturels p et q tels que pour tout n

$$(n > p) \Longrightarrow (|\alpha_n| < \sqrt{\varepsilon}),$$
$$(n > q) \Longrightarrow (|\beta_n| < \sqrt{\varepsilon}).$$

En posant $r = \sup(p, q)$ on voit que pour tout $n > r$ on a

$$(n > r) \Longrightarrow |\alpha_n\beta_n| < \varepsilon.$$

Donc $\lim(\alpha_n\beta_n) = 0$.
Revenons aux suites (a_n) et (b_n) nous avons pour tout n

$$a_n b_n = ab + a\,\beta_n + b\,\alpha_n + \alpha_n\beta_n.$$

La *suite constante* (ab) a pour *limite* ab,
la *suite* $(a\,\beta_n)$ a pour *limite* $a \times 0 = 0$,
la *suite* $(b\,\alpha_n)$ a pour *limite* $b \times 0 = 0$,
la *suite* $(\alpha_n\beta_n)$ a pour *limite* 0.
Donc la suite $(a_n b_n)$ somme de quatre suites convergentes est convergente et a pour limite $ab = (\lim a_n)(\lim b_n)$.
Concluons :

Théorème.

Quelles que soient les suites convergentes (a_n) et (b_n) et le nombre réel λ les suites $(a_n) + (b_n)$, $\lambda(a_n)$ et $(a_n)(b_n)$ sont convergentes et on a

$$\lim(a_n + b_n) = \lim a_n + \lim b_n.$$
$$\lim \lambda a_n = \lambda \lim a_n,$$
$$\lim a_n b_n = (\lim a_n)(\lim b_n).$$

Le résultat sur la limite de $(a_n)(b_n)$ s'étend par récurrence à k suites convergentes. En particulier pour tout entier $k \geqslant 2$ on a

$$\lim(a_n)^k = (\lim a_n)^k.$$

EXERCICES

(Cf. exercices 1. 2. 3. du § 3.15.)
On désigne par F l'ensemble des suites réelles convergentes.

1. Démontrer que F est un sous-groupe de $(S, +)$.
2. Démontrer que F est un sous-anneau de $(S, +, \times)$.
3. Démontrer que F est un sous-espace vectoriel de $(S, +, \cdot)$.

b) Somme et produit de suites tendant vers $+\infty$ (resp. $-\infty$) lorsque n tend vers $+\infty$.

Soit (a_n) une suite telle que $\lim a_n = +\infty$ et λ un nombre réel quelconque.
Quel que soit $A > 0$ et quel que soit n on a

$$(a_n + \lambda > A) \Longleftrightarrow (a_n > A - \lambda).$$

On en déduit

$$(\lim a_n = +\infty) \Longrightarrow (\lim (a_n + \lambda) = +\infty).$$

Vous démontrerez de même

$$(\lim a_n = -\infty) \Longrightarrow (\lim (a_n + \lambda) = -\infty).$$

Soit (a_n) et (b_n) deux suites telles que $\lim a_n = \lim b_n = +\infty$. Quel que soit $A > 0$ les deux relations

$$a_n > \frac{A}{2} \tag{3}$$

$$b_n > \frac{A}{2} \tag{4}$$

entraînent $a_n + b_n > A$. Or il existe des entiers naturels p et q tels que pour tout n de $\mathbb{N}$

$$(n > p) \Longrightarrow \left(a_n > \frac{A}{2}\right),$$

$$(n > q) \Longrightarrow \left(b_n > \frac{A}{2}\right).$$

En posant $r = \sup(p, q)$ on aura pour tout entier naturel n

$$(n > r) \Longrightarrow (a_n + b_n > A).$$

Donc $\lim (a_n + b_n) = +\infty$.
On démontrerait de même que si $\lim a_n = \lim b_n = -\infty$ alors $\lim (a_n + b_n) = -\infty$.

Lorsque n tend vers $+\infty$, si les deux suites (a_n) et (b_n) tendent vers $+\infty$ (resp. $-\infty$) alors la suite $(a_n + b_n)$ tend vers $+\infty$ (resp. $-\infty$).

EXERCICE

3. On définit les suites (a_n) (b_n) (c_n) (d_n) en posant pour tout n

$$a_n = n^2 + 1$$
$$b_n = n^2 + n$$
$$c_n = n^2 + (-1)^n$$
$$d_n = -n^3.$$

Démontrer que $\lim a_n = \lim b_n = \lim c_n = +\infty$, $\lim d_n = -\infty$; démontrer ensuite

$$\lim (a_n + d_n) = 1, \quad \lim (b_n + d_n) = +\infty$$

et enfin que $(c_n + d_n)$ n'a pas de limite « finie ou infinie ».

L'exercice précédent montre que *lorsque* $\lim a_n = +\infty$ et $\lim b_n = -\infty$ *on ne peut rien dire a priori sur la suite* $(a_n + b_n)$; *tous les cas peuvent se présenter.*
Pour l'étude des suites (λa_n) et $(a_n b_n)$ nous supposerons seulement $\lim |a_n| = \lim |b_n| = +\infty$.
Si $\lambda \neq 0$, quel que soit $A > 0$ on a

$$(|\lambda a_n| > A) \Longleftrightarrow \left(|a_n| > \frac{A}{|\lambda|}\right).$$

Il en résulte que $\lim |\lambda a_n| = +\infty$.

Quel que soit A les relations

(3′) $\qquad |a_n| > \sqrt{A}$

(4′) $\qquad |b_n| > \sqrt{A}$

entraînent $|a_n b_n| > A$. Or il existe des entiers naturels p et q tels que pour tout n

$$(n > p) \Longrightarrow (|a_n| > \sqrt{A}),$$
$$(n > q) \Longrightarrow (|b_n| > \sqrt{A}).$$

En posant $r = \sup(p, q)$ on aura pour tout entier naturel n

$$(n > r) \Longrightarrow (|a_n b_n| > A).$$

Concluons :

Lorsque n tend vers $+\infty$ si les suites $(|a_n|)$ et $(|b_n|)$ tendent vers $+\infty$, il en est de même de la suite $(|\lambda a_n|)$ pour $\lambda \neq 0$ et de la suite $(|a_n b_n|)$.

Lorsque les suites (a_n) et (b_n) tendent vers $+\infty$ ou $-\infty$ lorsque n tend vers $+\infty$, l'étude du signe de λa_n et de $a_n b_n$ montrera que (λa_n) et $(a_n b_n)$ tendent vers $+\infty$ ou bien vers $-\infty$.

c) Étude de l'inverse d'une suite.

Soit (u_n) une suite infinie réelle. On ne peut définir la suite $\left(\frac{1}{u_n}\right)$ que pour l'ensemble I des indices n tels que $u_n \neq 0$.

Premier cas : $\lim u_n = l \neq 0$.

Nous avons vu au § 3.18 c qu'il existe k de $\mathbb{N}$ tel que pour tout $n > k$ on ait

$$l - \frac{|l|}{2} < u_n < l + \frac{|l|}{2}$$

c'est-à-dire

si $l > 0$

$$0 < \frac{l}{2} < u_n < \frac{3l}{2}$$

si $l < 0$

$$\frac{3l}{2} < u_n < \frac{l}{2} < 0.$$

Dans les deux cas il existe *a strictement positif* tels que pour tout $n > k$ on ait

$$0 < a < |u_n| \quad \text{c'est-à-dire} \quad \left|\frac{1}{u_n}\right| < \frac{1}{a}.$$

Nous allons montrer que $\lim \frac{1}{u_n} = \frac{1}{l}$. *Donnons-nous* $\varepsilon > 0$ arbitrairement et cherchons n tel que

(5) $$\left|\frac{1}{u_n} - \frac{1}{l}\right| < \varepsilon$$

cette relation est équivalente à

(5′) $$\frac{|u_n - l|}{|u_n||l|} < \varepsilon.$$

Or

$$\frac{|u_n - l|}{|u_n||l|} < \frac{|u_n - l|}{a|l|}.$$

Donc l'inégalité

(6) $$\frac{|u_n - l|}{a|l|} < \varepsilon$$

équivalente à

(6') $$|u_n - l| < \varepsilon a |l|$$

entraîne pour tout $n > k$ la relation (5') donc aussi (5).

Nous savons qu'il existe un entier naturel p tel que pour tout $n > p$ on ait (6'). Posons $q = \sup(k, p)$, le raisonnement précédent montre que pour tout $n > q$ on aura l'inégalité (5). Donc $\lim\left(\frac{1}{u_n}\right) = \frac{1}{l}$.

Deuxième cas : $\lim u_n = 0$.

Nous supposerons qu'il existe un entier k tel que pour $n > k$ on ait $u_n \neq 0$.

Donnons-nous arbitrairement $A > 0$; pour tout $n > k$ on a

$$\left(\left|\frac{1}{u_n}\right| > A\right) \Longleftrightarrow \left(|u_n| < \frac{1}{A}\right).$$

Or il existe un entier p tel que pour tout $n > p$ on ait $|u_n| < \frac{1}{A}$; posons $q = \sup(k, p)$; pour tout $n > q$ on aura $\left|\frac{1}{u_n}\right| > A$; donc dans ce cas, $\lim\left|\frac{1}{u_n}\right| = +\infty$.

Troisième cas : $\lim |u_n| = +\infty$.

On voit immédiatement qu'il existe un entier k tel que pour tout $n > k$ on ait $|u_n| > 0$ c'est-à-dire $u_n \neq 0$. Quel que soit $\varepsilon > 0$ et pour tout $n > k$ on a

$$\left(\left|\frac{1}{u_n}\right| < \varepsilon\right) \Longleftrightarrow \left(|u_n| > \frac{1}{\varepsilon}\right).$$

Or il existe un entier p tel que pour tout $n > p$ on ait $|u_n| > \frac{1}{\varepsilon}$; posons $q = \sup(k, p)$; pour tout $n > q$ on aura $\left|\frac{1}{u_n}\right| < \varepsilon$; donc dans ce cas, $\lim \frac{1}{u_n} = 0$.

Concluons :

Si $\lim u_n = l \neq 0$ alors $\lim \frac{1}{u_n} = \frac{1}{l}$.

Si $\lim u_n = 0$ et s'il existe k tel que pour tout $n > k$ on ait $u_n \neq 0$ alors $\lim \left|\frac{1}{u_n}\right| = +\infty$.

Si $\lim |u_n| = +\infty$ alors $\lim \frac{1}{u_n} = 0$.

REMARQUE

Ces trois cas n'épuisent pas toutes les possibilités.

Le premier résultat ci-dessus et le résultat concernant le produit de deux suites convergentes permettent d'énoncer :

Si les deux suites (a_n) et (b_n) sont convergentes et si $\lim b_n \neq 0$ alors

$$\lim \frac{a_n}{b_n} = \frac{\lim a_n}{\lim b_n}.$$

d) Série géométrique.

Soit (aq^n) la **suite géométrique** de raison q et de terme d'indice zéro a. Nous supposerons $aq \neq 0$ sinon tous les termes sont nuls.
On appelle **série géométrique** la suite (S_n) définie pour tout n de $\mathbb{N}$ par

$$S_0 = a$$
$$S_1 = a + aq$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$S_n = a + aq + \ldots + aq^n.$$

Nous savons (cf. § 3.16b) que l'on a

si $q \neq 1$ $\qquad S_n = a\dfrac{1 - q^{n+1}}{1 - q} = \dfrac{a}{1 - q} - \dfrac{aq}{1 - q}\, q^n$

si $q = 1$ $\qquad S_n = (n + 1)\, a.$

Si $|q| < 1$ nous savons que $\lim q^n = 0$ (cf. 3.17d), donc d'après les résultats que nous venons d'obtenir nous avons

$$\lim S_n = \frac{a}{1 - q}.$$

Si $|q| > 1$ nous savons que $\lim |q^n| = +\infty$

donc

$$\lim |S_n| = +\infty.$$

Si $q = 1$ $S_n = (n + 1)\ a$ $(a \neq 0)$ donc $\lim |S_n| = +\infty.$

Si $q = -1$ $S_n = a\dfrac{1 - (-1)^{n+1}}{2} = a\dfrac{1 + (-1)^n}{2}$

c'est-à-dire

$$S_{2p} = a \neq 0 \quad \text{et} \quad S_{2p+1} = 0$$

la suite (S_n) est une suite dont l'ensemble des valeurs est $\{0, a\}$.

Théorème.

La suite (S_n) définie pour tout n de $\mathbb{N}$ par

$$S_n = a + aq + \ldots + aq^n$$

est convergente si et seulement si $|q| < 1$; on a alors

$$\lim S_n = \frac{a}{1 - q}.$$

On écrit dans ce cas ($|q| < 1$)

$$\sum_{n=0}^{n=+\infty} aq^n = \frac{a}{1-q}.$$

Il ne faut voir dans cette notation que la généralisation de la notation

$$S_n = \sum_{k=0}^{k=n} aq^k.$$

e) Exercices en partie résolus.

EXERCICE

5. *Soit deux suites* (u_n) *et* (v_n) *telles que*

$$\lim u_n = l \neq 0 \quad \text{et} \quad \lim |v_n| = +\infty$$

démontrer que lim $|u_n v_n| = +\infty$.

Comme au sous paragraphe *c*) on voit qu'il existe un réel $a > 0$ et un entier k tel que pour tout $n > k$ on ait

$$0 < a < |u_n|.$$

Donc $a|v_n| < |u_n v_n|$; donc pour tout $n > k$ on a quel que soit $A > 0$,

$$(a|v_n| > A) \Longrightarrow (|u_n v_n| > A).$$

Vous acheverez facilement la démonstration

Si $\lim u_n = l \neq 0$ et si $\lim |v_n| = +\infty$ alors
$\lim |u_n v_n| = +\infty$.

Si, à partir d'un certain rang, u_n et v_n ont des signes déterminés, on pourra conclure soit $\lim u_n v_n = +\infty$, soit $\lim u_n v_n = -\infty$.

EXERCICE

6. *Étudier la suite* (u_n) *définie pour tout n par*

$$u_n = -3n^4 + 2n^3 - n + 5.$$

Pour $n > 0$ on a

$$u_n = -3n^4\left(1 - \frac{2}{3}\frac{1}{n} + \frac{1}{3}\frac{1}{n^3} - \frac{5}{3}\frac{1}{n^4}\right)$$
$$= -3n^4 a_n.$$

On a $\lim(-3n^4) = -\infty$ et $\lim a_n = 1$ donc

$$\lim(-3n^4 + 2n^3 - n + 5) = -\infty.$$

D'une manière générale la suite u_n *définie pour tout* n *par*

$$u_n = a_h n^h + a_{h-1} n^{h-1} + \ldots + a_1 n + a_0$$

où $h \geqslant 1$ *et* $a_h \neq 0$, *a la même limite que la suite* $(a_h n^h)$ *c'est-à-dire*

si $a_h > 0$ alors $\lim u_n = +\infty$,

si $a_h < 0$ alors $\lim u_n = -\infty$.

EXERCICE

7. *Étudier les suites* (u_n), (v_n), (w_n) :

$$u_n = \frac{-3n^3 - n + 1}{2n^2 - n}, \quad v_n = \frac{2n - 3}{7n^2 - 3n + 2}, \quad w_n = \frac{4n^3 - 5n^2 + 3}{-2n^3 + 2n - 1}$$

(chacune d'elle étant définie pour tout n strictement supérieur à toutes les racines de son dénominateur).

Vous démontrerez sans peine que les égalités

$$u_n = \frac{-3n^3}{2n^2} \frac{1 + \frac{1}{3n^2} - \frac{1}{3n^3}}{1 - \frac{1}{2n}},$$

$$v_n = \frac{2n}{7n^2} \frac{1 - \frac{3}{2n}}{1 - \frac{3}{7n} + \frac{2}{7n^2}},$$

$$w_n = \frac{4n^3}{-2n^3} \frac{1 - \frac{5}{4n} + \frac{3}{4n^3}}{1 - \frac{1}{n^2} + \frac{1}{2n^3}},$$

permettent de conclure

$$\lim u_n = -\infty,$$
$$\lim v_n = 0,$$
$$\lim w_n = -2.$$

D'une manière générale si on pose

$$u_n = \frac{a_h n^h + \ldots + a_1 n + a_0}{b_k n^k + \ldots + b_1 n + b_0} \qquad (h, k \in \mathbb{N},\ a_k \neq 0,\ b_k \neq 0)$$

pour tout n strictement supérieur à toutes les racines du dénominateur, on verra que la suite (u_n) a la même limite que la suite $\left(\frac{a_h n^h}{b_k n^k}\right)$ c'est-à-dire

si $h > k$ $\quad \lim |u_n| = +\infty$ $\quad \left(\text{avec le signe de } \frac{a_h}{b_k}\right)$,

si $h < k$ $\quad \lim u_n = 0$ $\quad \left(\text{avec le signe de } \frac{a_h}{b_k}\right)$,

si $h = k$ $\quad \lim u_n = \frac{a_h}{b_k}$.

V. Calculs approchés

Les calculs approchés s'effectuant généralement à l'aide de la numération décimale nous commencerons par étudier les nombres décimaux et la représentation décimale des nombres réels. Nous verrons d'ailleurs comment les résultats obtenus peuvent être transposés lorsque l'on utilise la numération de base a.

3. 20 NOMBRES DÉCIMAUX. ÉCRITURE DÉCIMALE DES DÉCIMAUX

a) Nombres décimaux.

On appelle **nombre décimal** d tout rationnel égal au quotient d'un entier relatif A par une puissance entière positive de 10.

Si $\mathbb{D}$ désigne l'ensemble des nombres décimaux, on voit qu'un rationnel x appartient à $\mathbb{D}$ si et seulement s'il existe A de $\mathbb{Z}$ et $k \in \mathbb{N}$ tel que

$$x = A\ 10^{-k}.$$

On voit alors que l'on a

$$\mathbb{Z} \subset \mathbb{D} \subset \mathbb{Q}.$$

Le dénominateur de la fration $\frac{A}{10^k}$ ne contient que les facteurs 2 et 5 (facteurs premiers de 10). Il existe donc un entier A′ non divisible par 2 ou par 5 tel que

$$A\ 10^{-k} = A'\ 2^{-p}\ 5^{-q},$$

où p et q sont deux entiers naturels; la fraction $\frac{A'}{2^p 5^q}$ est *irréductible*.

Réciproquement soit un nombre rationnel représenté par la *fraction irréductible* $\frac{A'}{2^p 5^q}$ ($A' \in \mathbb{Z}$, $p \in \mathbb{N}$, $q \in \mathbb{N}$) on aura :

si $p \leqslant q$ $\qquad \frac{A'}{2^p 5^q} = \frac{A' 2^{q-p}}{2^q 5^q} = \frac{A' 2^{q-p}}{10^q} \in \mathbb{D},$

si $q < p$ $\qquad \frac{A'}{2^p 5^q} = \frac{A' 5^{p-q}}{2^p 5^p} = \frac{A' 5^{p-q}}{10^p} \in \mathbb{D}.$

Concluons :

> Un nombre rationnel est décimal si et seulement si la fraction irréductible à dénominateur positif qui le représente est telle que ce dénominateur ne contienne que les facteurs 2 et 5.

EXERCICES

1. Démontrer que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$ considéré comme anneau.
2. Quels sont les décimaux dont l'inverse est un décimal ? Démontrer que leur ensemble est un sous-groupe du groupe $(\mathbb{Q}^*, \times)$.

b) Écriture décimale d'un décimal.

Soit $d = A\ 10^{-k}$, supposons d'abord d **positif** ; on a donc $A \in \mathbb{N}$ et $k \in \mathbb{N}$.
En numération décimale A s'écrira

$$A = \overline{\alpha_h \alpha_{h-1} \ldots \alpha_1 \alpha_0}$$

où $\alpha_h, \ldots, \alpha_0$ appartiennent à $\{0, 1, 2, \ldots, 9\}$; ce qui signifie

$$A = \alpha_h\ 10^h + \alpha_{h-1}\ 10^{h-1} \ldots + \alpha_1\ 10 + \alpha_0.$$

L'écriture décimale de $A\ 10^{-k} \geqslant 0$ est définie par les règles suivantes.

Premier cas : $k \leqslant h$. On place une virgule *avant les k derniers chiffres de* A.

$$A\ 10^{-k} = \overline{\alpha_h \ldots \alpha_k, \alpha_{k-1} \ldots \alpha_0}.$$

Par exemple

$$317 \times 10^{-1} = 31{,}7 \qquad 13\,580 \times 10^{-4} = 1{,}3580.$$

Deuxième cas : $h < k$. Vous savez que sans modifier la valeur de l'entier écrit sous forme décimale on peut placer à sa gauche un ou plusieurs chiffres zéro.
On placera $k - h$ chiffres 0 avant l'écriture décimale de A et on place une virgule avant les k derniers chiffres de A ainsi écrit

$$A\ 10^{-k} = \overline{0{,}\underbrace{00 \ldots 0}_{k \text{ chiffres}}\ \alpha_h \ldots \alpha_0}.$$

Attention! Le nombre de chiffres de $A = \alpha_h \ldots \alpha_1\alpha_0$ est $h + 1$ si vous faites intervenir ce nombre h' de chiffres il faut écrire $k - h' + 1$ chiffres zéro avant l'écriture de A. Par exemple

$$27 \times 10^{-2} = 0{,}27 \qquad 1\,972 \times 10^{-7} = 0{,}0001972.$$

Changeons de notation; un nombre décimal positif s'écrira donc dans le système décimal

$$d = \overline{\alpha_{-m} \ldots \alpha_{-1}\alpha_0, \alpha_1\alpha_2 \ldots \alpha_n}$$

où $\alpha_{-m}, \ldots \alpha_0, \alpha_1, \ldots, \alpha_n$ appartiennent à $\{0, 1, 2, \ldots, 9\}$. Les chiffres $\alpha_1, \alpha_2, \ldots, \alpha_n$ sont les **décimales** de d, ce sont les chiffres écrits après la virgule; α_k est la $k^{\text{ième}}$ décimale de d.

Il y a n décimales dans l'écriture ci-dessus de d; d'après les conventions adoptées pour l'écriture de d on a

$$\begin{aligned} A = d \times 10^n &= \overline{\alpha_{-m} \ldots \alpha_0\alpha_1 \ldots \alpha_n} \\ &= \alpha_{-m}\, 10^{m+n} + \ldots + \alpha_0\, 10^n + \alpha_1\, 10^{n-1} + \ldots + \alpha_n \end{aligned}$$

donc

(1) $$\boxed{\overline{\alpha_{-m} \ldots \alpha_0, \alpha_1 \ldots \alpha_n} = \alpha_{-m}10^m + \ldots + \alpha_0 + \alpha_1 10^{-1} + \ldots + \alpha_n 10^{-n} = \sum_{k=-m}^{k=n} \alpha_k 10^{-k}}$$

Ainsi donc c'est la *place de la virgule* qui fixe la valeur représentée par chaque chiffre de l'écriture décimale de d.

Enfin si d est **négatif** l'écriture décimale de d s'obtient en faisant précéder du signe — l'écriture décimale de $-d$, ainsi

$$\begin{aligned} -(328 \times 10^{-2}) &= -3{,}28 \\ -(708 \times 10^{-5}) &= -0{,}00708 \end{aligned}$$

La formule (1) permet de légitimer les règles des opérations sur les décimaux : addition, multiplication, calcul des valeurs approchées à 10^{-k} près, comparaison. Nous rappellerons ci-dessous deux de ces règles dont nous aurons besoin dans la suite.

Remarquons immédiatement que la formule (1) montre que l'on peut placer un ou plusieurs zéros avant α_{-m} et après α_n sans modifier la valeur du décimal ainsi écrit; aussi on a

$$\begin{aligned} &123{,}27 = 123{,}270 = 123{,}2700 = \ldots = 0123{,}27 = \ldots \\ &-5{,}109 = -5{,}1090 = -5{,}10900 = \ldots = -05{,}109 = -005{,}109 \ldots \end{aligned}$$

Cette introduction de zéros est parfois nécessaire dans certaines opérations. Étant donnés deux décimaux d et d' elle permet de les écrire

$$\begin{aligned} d &= \varepsilon\ \overline{\alpha_{-m} \ldots \alpha_0, \alpha_1 \ldots \alpha_n} \quad \text{où} \quad \varepsilon = +1 \text{ ou bien } -1, \\ d' &= \varepsilon'\ \overline{\alpha'_{-m} \ldots \alpha'_0, \alpha'_1 \ldots \alpha'_n} \quad \text{où} \quad \varepsilon' = +1 \text{ ou bien } -1. \end{aligned}$$

c) Multiplication d'un décimal par 10^p. Applications.

La formule (1) montre que pour multiplier un décimal par 10^p il suffit de déplacer la virgule

de p rangs vers la droite si $p > 0$,
de p rangs vers la gauche si $p < 0$;

éventuellement il aura fallu ajouter des zéros après α_n ou avant α_{-m}.

Exemples :

$$10^3 \times 12{,}7095 = 12\,709{,}5$$
$$10^{-2} \times (-328{,}4) = -3{,}284$$
$$10^4 \times 24{,}3 = 10^4 \times 24{,}3000 = 243\,000$$
$$10^{-5} \times 13 = 10^{-5} \times 000013 = 0{,}00013.$$

d) Comparaison des décimaux. Valeurs approchées à 10^{-k} près ($k \in \mathbb{N}$).

Il suffit de savoir comparer deux décimaux positifs : en effet si $d \leqslant 0$ et $d' \geqslant 0$ on a $d \leqslant d'$; si d et d' sont négatifs ils sont dans l'ordre opposé à celui présenté par $-d$ et $-d'$.

Soit donc d et d' *positifs*; posons

$$d = \overline{\alpha_{-m} \ldots \alpha_0, \alpha_1 \ldots \alpha_n}$$
$$d' = \overline{\alpha'_{-m} \ldots \alpha'_0, \alpha'_1 \ldots \alpha'_n}$$

les décimaux d et d' sont dans le même ordre que les entiers naturels

$$10^n d = \overline{\alpha_{-m} \ldots \alpha_0 \alpha_1 \ldots \alpha_n}$$
$$10^n d' = \overline{\alpha'_{-m} \ldots \alpha'_0 \alpha'_1 \ldots \alpha'_n}.$$

Conformément à ce que nous avons vu au chapitre 1er il suffit de comparer à partir de la gauche les différents chiffres. *Donc $d < d'$ si et seulement si*

$$\alpha_{-m} < \alpha'_{-m}$$

ou il existe un entier k ($-m < k < n$) tel que

$$(\forall\, h \in [-m, k]) \quad \alpha_h = \alpha'_h \quad \text{et} \quad \alpha_{k+1} < \alpha'_{k+1}.$$

De même $d = d'$ si et seulement si

$$(\forall\, h \in [-m, n]) \qquad \alpha_h = \alpha'_h.$$

En particulier quels que soient les chiffres $\alpha_1 \ldots \alpha_n$

$$0 \leqslant \overline{0, \alpha_1 \alpha_2 \ldots \alpha_n} < 1 \tag{2}$$

et plus généralement quels que soient les chiffres $\alpha_{k+1} \ldots \alpha_n$

$$0 \leqslant \overline{0, \underbrace{0 \ldots 0}_{k \text{ zéros}} \alpha_{k+1} \ldots \alpha_n} < 10^{-k}. \tag{3}$$

Ces inégalités vont nous permettre, connaissant la représentation décimale d'un décimal d, de trouver ses **valeurs approchées par défaut et par excès à 10^{-k} près** ($k \in \mathbb{N}$).

Rappelons que pour tout réel x et tout entier $k \geqslant 0$ (cf. § 3.14c) il existe un entier p_k *unique* tel que

$$p_k \leqslant 10^k x < p_k + 1;$$

p_k est la partie entière de $10^k x$; on a

$$p_k\, 10^{-k} \leqslant x < (p_k + 1)\, 10^{-k}$$

$a_k = p_k\, 10^{-k}$ est appelé valeur approchée par défaut à 10^{-k} près de x,
$b_k = (p_k + 1)\, 10^{-k}$ est appelé valeur approchée par excès à 10^{-k} près de x.

On dit aussi que a_k et b_k sont les **valeurs approchées décimales d'ordre** k; elles sont *uniques*; par abus de langage, on dira plus simplement que ce sont les **valeurs approchées d'ordre** k.

Supposons d'abord d **positif.** Nous avons

$$d = \overline{\alpha_{-m} \dots \alpha_{-1}\alpha_0, \alpha_1 \dots \alpha_n}.$$

D'après la formule (1) on a

$$d = \overline{\alpha_{-m} \dots \alpha_0} + \overline{0, \alpha_1 \dots \alpha_n}$$

avec

$$p_0 = \overline{\alpha_{-m} \dots \alpha_0} \in \mathbb{N} \quad \text{et} \quad 0 \leqslant \overline{0, \alpha_1 \dots \alpha_n} < 1$$

donc

$$p_0 \leqslant d < p_0 + 1$$

p_0 est donc la **partie entière** du décimal d.

De même la formule (1) nous permet d'écrire pour $k < n$

$$d = a_k + \overline{0{,}0 \dots 0\, \alpha_{k+1} \dots \alpha_n}$$

avec

$$a_k = \overline{\alpha_{-m} \dots \alpha_0, \alpha_1 \dots \alpha_k} = p_k\, 10^{-k} \qquad (p_k \in \mathbb{N})$$

et

$$0 \leqslant \overline{0, 0 \dots 0\, \alpha_{k+1} \dots \alpha_n} < 10^{-k}$$

donc

$$a_k = p_k\, 10^{-k} \leqslant d < (p_k + 1)\, 10^{-k} = a_k + 10^{-k};$$

par conséquent a_k est la *valeur approchée par défaut à* 10^{-k} *près du décimal* d; $b_k = a_k + 10^{-k}$ est sa valeur approchée par excès à 10^{-k} près.

Si $k \geqslant n$ on voit que l'on a

$$a_k = a_n = d$$

et on aura $b_k = a_k + 10^{-k} = d + 10^{-k}$.

Exemple $d = 35{,}1049$

k	$a_k = p_k 10^{-k}$	$b_k = (p_k + 1)\, 10^{-k}$
0	35	36
1	35,1	35,2
2	35,10	35,11
3	35,104	35,105
4	35,1049	35,1050
5	35,10490	35,10491
6	35,104900	35,104901
.	.	.
.	.	.
.	.	.

Si d est **négatif**, il faut faire attention car, si on désigne par a_k et b_k les valeurs approchées à 10^{-k} près de $-d$, on a

$$a_k \leqslant -d < b_k$$

d'où

$$-b_k < d \leqslant -a_k.$$

Si $-b_k < d < -a_k$, aucun problème, $-b_k$ est la valeur approchée *par défaut* à 10^{-k} près de d.
Mais si $d = -a_k$ cette valeur approchée *par défaut* à 10^{-k} près est $-a_k$.

EXERCICE

3. Trouver pour $0 \leqslant k \leqslant 6$ les valeurs approchées par défaut et par excès à 10^{-k} près de $d' = -35{,}1049$.

Remarque sur les notations.

Désormais nous ne surlignerons plus l'écriture décimale d'un nombre décimal.
Si $d = \alpha_{-m} \ldots \alpha_0, \alpha_1 \ldots \alpha_n \geqslant 0$, nous avons

$$d = p_0 + 0, \alpha_1 \ldots \alpha_n.$$

Nous l'écrirons simplement

$$d = p_0, \alpha_1\alpha_2 \ldots \alpha_n$$

c'est un abus de notation : p_0 est *supposé être écrit en notation décimale.*
On a donc

$$d = p_0 + \frac{\alpha_1}{10} + \frac{\alpha_2}{10^2} + \ldots + \frac{\alpha_n}{10^n}$$

p_0 est la **partie entière** de $d \geqslant 0$ et $0, \alpha_1 \ldots \alpha_n$ la **partie décimale.**
Si $d < 0$ et si $-d = p_0, \alpha_1 \ldots \alpha_n$ nous écrirons

$$d = -(p_0, \alpha_1 \ldots \alpha_n)$$

mais dans ce cas on a

$$\begin{aligned} d = -p_0 - 0, \alpha_1 \ldots \alpha_n &= -(p_0 + 1) + (1 - 0, \alpha_1 \ldots \alpha\ ) \\ &= -(p_0 + 1) + 0, \alpha'_1 \ldots \alpha'_n \end{aligned}$$

donc si $d = -(p_0, \alpha_1 \ldots \alpha_n)$ la partie entière est $-(p_0 + 1)$ et non $-p_0$.

REMARQUE

Dans certains calculs, en particulier dans les *calculs logarithmiques* au lieu d'écrire $d = -(p_0, \alpha_1 \ldots \alpha_n)$ on écrit le décimal

$$d = -(p_0 + 1) + 0, \alpha'_1 \ldots \alpha'_n$$

sous la forme

$$d = \overline{p_0 + 1}, \alpha'_1 \ldots \alpha'_n$$

où $\overline{p_0 + 1}$ signifie $-(p_0 + 1)$ qui est appelé la **caractéristique** de d. Le nombre $0, \alpha'_1, \ldots \alpha'_n$ est alors appelé la **mantisse** de d et on a $0 \leqslant 0, \alpha'_1, \ldots \alpha'_n < 1$.

Exemples :

$$-(3{,}14904) = -4 + (1 - 0{,}14904) = \overline{4}{,}85096$$
$$-(0{,}027) = \overline{1}{,}973$$
$$-(127{,}94000) = \overline{128}{,}06000.$$

3. 21 REPRÉSENTATION D'UN NOMBRE RÉEL PAR UN DÉVELOPPEMENT DÉCIMAL ILLIMITÉ

a) Propriétés des valeurs approchées à 10^{-n} près ($n \in \mathbb{N}$) d'un nombre réel.

Quel que soit le réel x et quel que soit l'entier naturel n il existe un **entier unique** p_n tel que

(1) $$p_n\, 10^{-n} \leqslant x < (p_n + 1)\, 10^{-n}$$

Le décimal $a_n = p_n\, 10^{-n}$, **valeur approchée par défaut à 10^{-n} près** de x est **le plus grand** multiple entier de 10^{-n} **inférieur** à x.
Le décimal $b_n = (p_n + 1)\, 10^{-n}$, **valeur approchée par excès à 10^{-n} près** de x est **le plus petit** multiple entier de 10^{-n} **strictement supérieur** à x.
Ces nombres décimaux de la forme $A\, 10^{-n}$ ($A \in \mathbb{Z}$) sont **uniques.**

REMARQUE

1. Tout nombre réel x' tel que $a_n \leqslant x' \leqslant x$ est *une* valeur approchée par défaut de x vérifiant $x - x' \leqslant 10^{-n}$. Lorsque l'on parle de *la* valeur approchée par défaut d'ordre n de x il s'agit *du nombre décimal unique* $p_n\, 10^{-n}$ ($p_n \in \mathbb{Z}$).

Les nombres décimaux a_n et b_n sont encore appelées **valeurs approchées décimales d'ordre** n de x.
Pour $n + 1$ nous avons

(2) $$p_{n+1}\, 10^{-(n+1)} \leqslant x < (p_{n+1} + 1)\, 10^{-(n+1)},$$

et la relation (1) peut s'écrire

(1') $$(10\, p_n)\, 10^{-(n+1)} \leqslant x < [10\, (p_n + 1)]\, 10^{-(n+1)}.$$

Les décimaux $p_{n+1}\, 10^{-(n+1)}$ et $(10\, p_n)\, 10^{-(n+1)}$ sont deux multiples entiers de $10^{-(n+1)}$ inférieurs à x; donc $p_{n+1}\, 10^{-(n+1)}$, valeur approchée par défaut à $10^{-(n+1)}$ près de x, est *le plus grand* de ces deux décimaux et on a pour tout n

$$a_n \leqslant a_{n+1}.$$

De même les décimaux $(p_{n+1} + 1)\, 10^{-(n+1)}$ et $10\, (p_n + 1)\, 10^{-(n+1)}$ sont deux multiples entiers de $10^{-(n+1)}$ strictement supérieurs à x; donc $(p_{n+1} + 1)\, 10^{-(n+1)}$, valeur approchée par excès à $10^{-(n+1)}$ près de x, est *le plus petit* de ces deux décimaux et on a

$$b_{n+1} \leqslant b_n.$$

Ceci va nous permettre d'étudier les deux suites infinies réelles (a_n) et (b_n).
Pour tout n on a en effet

$$a_n \leqslant a_{n+1} \leqslant x < b_{n+1} \leqslant b_n$$
$$b_n - a_n = 10^{-n}.$$

Comme $0 < \frac{1}{10} < 1$ on a $\lim (b_n - a_n) = 0$; par conséquent les suites (a_n) et (b_n) sont *deux suites adjacentes* et on a (cf.§ 3.17 a, exemple 4)

$$\lim a_n = \lim b_n = x.$$

Théorème.

Pour tout réel x la suite (a_n) de ses valeurs approchées par défaut à 10^{-n} près et la suite (b_n) de ses valeurs approchées par excès à 10^{-n} près sont des suites adjacentes ayant pour limite commune ce nombre x.

REMARQUE

2. Pour un nombre décimal $x = A\,10^{-k}$ ($A \in \mathbb{Z}$, $k \in \mathbb{N}$) ces propriétés énoncées dans le théorème sont triviales car la suite (a_n) est une suite stationnaire; en effet pour tout $n \geqslant k$ on a

$$a_n = a_k = x$$

C'est pour cela que nous n'avions pas énoncé ce théorème pour les nombres x décimaux au § 3.20 b.

Les décimaux étant des rationnels nous pouvons énoncer

Corollaire.

Tout nombre réel est limite d'une suite infinie (r_n) de nombres rationnels.

b) Représentation d'un nombre réel par un développement décimal illimité.

Désignons toujours par a_n et b_n les valeurs approchées par défaut et par excès à 10^{-n} près d'un réel quelconque x.

Pour tout entier h tel que $0 \leqslant h < n$ on a

$$a_h \leqslant a_n \leqslant x < b_n \leqslant b_h,$$

d'où

$$a_h \leqslant a_n < b_h$$

donc, comme $b_h = a_h + 10^{-h}$, a_h est la valeur approchée par défaut d'ordre h de a_n valeur approchée par défaut d'ordre n de x.

Cette remarque va nous permettre d'associer un développement décimal « illimité » à tout réel x.

Supposons d'abord x **positif.**

La propriété que nous venons de démontrer et l'écriture décimale des valeurs approchées d'un décimal (cf. § 3.19d) d'ordre n nous montre que l'on a

$$\begin{array}{ll}
a_0 = p_0 \in \mathbb{N} & b_0 = p_0 + 1 \\
a_1 = p_0, \alpha_1 & b_1 = p_0, \alpha_1 + 10^{-1} \\
a_2 = p_0, \alpha_1\alpha_2 & b_2 = p_0, \alpha_1\alpha_2 + 10^{-2} \\
\cdot & \\
\cdot & \\
\cdot & \\
a_n = p_0, \alpha_1\alpha_2 \ldots \alpha_n & b_n = p_0, \alpha_1\alpha_2 \ldots \alpha_n + 10^{-n} \\
a_{n+1} = p_0, \alpha_1\alpha_2 \ldots \alpha_n\alpha_{n+1} & b_{n+1} = p_0, \alpha_1\alpha_2 \ldots \alpha_n\alpha_{n+1} + 10^{-(n+1)} \\
\cdot & \cdot \\
\cdot & \cdot \\
\cdot & \cdot
\end{array}$$

où l'entier naturel p_0 *est supposé écrit en numération décimale* et où pour tout $n \in \mathbb{N}^*$ on a

$$\alpha_n \in \{0, 1, 2, \ldots, 9\}.$$

Au lieu d'écrire

$$x = \lim_{n \to +\infty} p_0, \alpha_1\alpha_2 \ldots \alpha_n$$

nous conviendrons d'écrire ($x \geqslant 0$)

$$x = p_0, \alpha_1\alpha_2 \ldots \alpha_n \ldots$$

et nous dirons que $p_0, \alpha_1\alpha_2 \ldots \alpha_n \ldots$ est le **développement décimal illimité** du réel positif x.

Si x est **négatif** et si

$$-x = p_0, \alpha_1\alpha_2 \ldots \alpha_n \ldots$$

nous conviendrons d'écrire

$$x = -p_0, \alpha_1\alpha_2 \ldots \alpha_n \ldots$$

On dit aussi que ce développement est une **suite décimale illimitée**; en fait deux suites infinies interviennent dans cette étude la suite infinie décimale (a_n) et la suite infinie $(\alpha_n)_{n\in\mathbb{N}^*}$ prenant ses valeurs dans $\{0, 1, 2, \ldots, 9\}$.
Avec ces conventions nous voyons qu'un nombre décimal $d = A\,10^{-k}$ $(A \in \mathbb{Z}, k \in \mathbb{N})$ peut s'écrire

$$d = \varepsilon\, p_0, \alpha_1\alpha_2 \ldots \alpha_k\, 000 \ldots \quad (\varepsilon = +1 \quad \text{ou} \quad \varepsilon = -1).$$

c) Étude de la réciproque.

Dans l'étude précédente c'est la connaissance de x qui permet de déterminer $p_0 \in \mathbb{N}$ et la suite $(\alpha_n)_{n\in\mathbb{N}^*}$ dont les valeurs appartiennent à $\{0, 1 \ldots, 9\}$.
Réciproquement donnons-nous arbitrairement $p_0 \in \mathbb{N}$ et une telle suite $(\alpha_n)_{n\in\mathbb{N}^*}$ posons

$$a'_0 = p_0$$

et $$(\forall n \in \mathbb{N}^*) \qquad a'_n = p_0, \alpha_1 \ldots \alpha_n$$

Cherchons si la suite infinie réelle (a'_n) a une limite. Posons $b'_n = a'_n + 10^{-n}$.
Nous avons déjà pour tout n

$$b'_n - a'_n = 10^{-n} > 0$$
$$0 \leqslant a'_{n+1} - a'_n = \alpha_{n+1}\, 10^{-(n+1)} \leqslant 9 \times 10^{-(n+1)},$$

d'autre part pour tout n on a

$$b'_n - b'_{n+1} = a'_n + 10^{-n} - a'_{n+1} - 10^{-(n+1)}$$
$$= (9 - \alpha_{n+1})\, 10^{-(n+1)} \geqslant 0$$

Donc pour tout n on a

$$\begin{cases} a'_n \leqslant a'_{n+1} < b'_{n+1} \leqslant b'_n \\ b'_n - a'_n = 10^{-n} \end{cases}$$

Les deux suites (a'_n) et (b'_n) sont donc adjacentes, elles ont donc pour limite commune un nombre réel x.

REMARQUE

3. Nous trouvons $x' \geqslant 0$ parce que nous sommes partis de la suite (a'_n) où $a'_n \geqslant 0$ pout tout n, en considérant la suite $(-a'_n)$ nous obtiendrons comme limite de la suite $(-a'_n)$ le nombre réel $-x \leqslant 0$.

Nous dirons que $p_0, \alpha_1 \ldots \alpha_n \ldots$ est *un* développement décimal illimité égal à x. Rien ne prouve que si l'on cherchait le développement décimal illimité de x obtenu en b) à l'aide des valeurs approchées d'ordre n de x on retrouverait $p_0, \alpha_1 \ldots \alpha_n \ldots$; nous allons étudier cette question ci-dessous.

d) Complément. Étude de l'unicité du développement décimal illimité d'un nombre réel.

Nous utiliserons dans cette étude certains des résultats donnés dans les § 3.18 et 3.19.
On remarquera la différence des démarches effectuées dans les sous-paragraphes b) et c). Dans b) on part de $x \in \mathbb{R}$ et à l'aide des valeurs approchées par défaut à 10^{-n} près de x on trouve un développement décimal illimité représentant x.

Dans c) on se donne a priori un développement décimal illimité et on montre que ce développement permet de définir une suite (a'_n) de nombres décimaux $a'_n = p'_n 10^{-n}$ qui a pour limite un nombre réel x; *mais on ne sait pas si a'_n est la valeur approchée de x à 10^{-n} près.* Autrement dit on ne sait pas si, en appliquant à ce nombre x le processus du sous-paragraphe b) on ne trouverait pas pour x un développement décimal illimité distinct du développement dont on est parti.

En revanche si on peut démontrer que le *nombre décimal a_n considéré au sous-paragraphe c) est, pour tout n, la valeur approchée à 10^{-n} près du nombre réel x*, on pourra affirmer qu'à ce nombre x on peut associer un *développement décimal illimité unique* puisque ce développement est obtenu à partir de la suite décimale (a_n) des valeurs approchées par défaut à 10^{-n} près, suite qui, comme on le sait, est unique.

Un exemple nous montrera que cette propriété n'est pas vraie pour tout x.

EXEMPLE

Posons

$$x = 0{,}99\ldots9\ldots$$

c'est-à-dire $p = 0$ et pour tout $n > 0$ $\alpha_n = 9$.

On aura

$$a'_0 = 0$$

et pour tout $n \geqslant 1$ (cf. § 3.16 b)

$$a'_n = 9 \times 10^{-1} + \ldots + 9 \times 10^{-n} = 9 \times 10^{-1}(1 + 10^{-1} + \ldots + 10^{-(n-1)})$$

$$= 9 \times 10^{-1} \frac{1 - 10^{-n}}{1 - 10^{-1}} = 1 - 10^{-n}$$

donc

$$x = \lim a'_n = 1.$$

On a donc $x = 1, 0\ldots0\ldots$ développement décimal illimité de 1 obtenu avec les valeurs approchées par défaut d'ordre n et $x = 0{,}9\ 9\ldots9\ldots$ appelé *développement impropre de x.*

Dans l'étude du sous paragraphe c) le décimal a'_k sera la valeur approchée à 10^{-k} près par défaut de x si et seulement si

$$a'_k \leqslant x < a'_k + 10^{-k}.$$

Nous avons pour tout $n > k$

$$a'_n = p_0, \alpha_1 \ldots \alpha_k \ldots \alpha_n = p_0 + \sum_{i=1}^{i=k} \alpha_i 10^{-i} + \sum_{j=k+1}^{j=n} \alpha_j 10^{-j}$$

c'est-à-dire

$$a'_n = a'_k + \sum_{j=k+1}^{j=n} \alpha_j 10^{-j};$$

l'entier *k étant fixé* nous avons (cf § 3.19 a)

$$x = \lim_{n \to +\infty} a'_n = a'_k + \lim_{n \to +\infty} \sum_{j=k+1}^{j=n} \alpha_j 10^{-j}.$$

Deux cas peuvent se présenter

1. *Ou bien pour tout $n > k$ on a* $\alpha_n = 9$.

On a alors (cf. § 3.16 b)

$$\sum_{j=k+1}^{j=n} \alpha_j 10^{-j} = 9 \times 10^{-(k+1)} + \ldots + 9 \times 10^{-n}$$
$$= 9 \times 10^{-(k+1)} (1 + 10^{-1} + \ldots + 10^{-(n-k-1)})$$
$$= 9 \times 10^{-(k+1)} \frac{1 - 10^{-(n-k)}}{1 - 10^{-1}}$$
$$= 10^{-k} (1 - 10^{-(n-k)}).$$

Lorsque n tend vers $+\infty$, ou lorsque $n - k$ tend vers $+\infty$, puisque k est fixé, nous savons (cf. § 3.19 d) que ce nombre tend vers 10^{-k}; il en résulte que

$$x = a'_k + 10^{-k}.$$

Donc dans ce cas ($\alpha_n = 9$ pour tout $n > k$) le décimal a'_k n'est pas égal à la valeur approchée par défaut d'ordre k du nombre x. Cette valeur a_k est égale à $a'_k + 10^{-k}$.

2. *Il existe $h > k$ tel que $\alpha_h < 9$.*

Pour tout $n > k$ posons $\sum_{j=k+1}^{j=n} \alpha_j 10^{-j} = u_n$; remplacons dans u_n tous les α_j où $j \neq h$ par 9 et laissons α_h nous obtenons

$$u_n \leqslant u'_n = \left(\sum_{j=k+1}^{j=h-1} 9 \times 10^{-j} \right) + \alpha_h 10^{-h} + \left(\sum_{j=h+1}^{j=n} 9 \times 10^{-j} \right).$$

D'autre part

$$u'_n = \left(\sum_{j=k+1}^{j=n} 9 \times 10^{-j} \right) - (9 - \alpha_h) 10^{-h}$$

donc d'après ce que nous avons vu ci-dessus

$$\lim_{n \to +\infty} u'_n = 10^{-k} - (9 - \alpha_h) \quad 10^{-h}$$

et comme $9 - \alpha_h > 0$ on a $\lim u'_n < 10^{-k}$. Donc

$$\lim_{n \to +\infty} \sum_{j=k+1}^{j=n} \alpha_j 10^{-j} \leqslant \lim_{n \to +\infty} u'_n < 10^{-k}$$

et par conséquent dans ce cas ($\alpha_h < 9$)

$$x - a'_k < 10^{-k}$$

donc a'_k est bien la valeur approchée décimale par défaut d'ordre k de x.

Nous pouvons maintenant étudier l'*unicité* du développement décimal d'un nombre réel x. Supposons que l'on ait

$$x = p_0, \alpha_1 \ldots \alpha_n \ldots \qquad (p_0 \in \mathbb{N}, \alpha_n \in \{0, 1, \ldots, 9\}).$$

Premier cas. *Il existe une infinité de valeurs de n telles que $\alpha_n < 9$.*

Quel que soit l'entier naturel k il existera toujours $h > k$ tel que $\alpha_h < 9$; donc pour tout k de $\mathbb{N}$

$$a'_k = p_0, \alpha_1 \ldots \alpha_k$$

est la *valeur approchée par défaut d'ordre k de x.*

En cherchant le développement décimal illimité de x par les valeurs approchées d'ordre k nous retrouverions $p_0, \alpha_1 \ldots \alpha_n \ldots$. Ce nombre x est représenté par un développement décimal illimité unique.

Deuxième cas. *Il existe k de $\mathbb{N}$ tel que pour tout $n > k$ on ait $\alpha_n = 9$.*

Dans ce cas

$$x = a'_k + 10^{-k}.$$

c'est le nombre décimal

$$x = p_0, \alpha_1 \ldots \alpha_k + 10^{-k}$$

Si $\alpha_k < 9$ on pourra écrire

$$x = p_0, \alpha_1 \ldots \alpha_{k-1} (\alpha_k + 1)\, 0 \ldots 0 \ldots .$$

et

$$x = p_0, \alpha_1 \ldots \alpha_k\, 9 \ldots 9 \ldots .$$

Le deuxième développement, celui dont nous sommes partis, est appelé développement *décimal illimité impropre* du décimal x.

Dans cette étude nous avons supposé $x \geqslant 0$; pour $x \leqslant 0$ les résultats subsistent; il suffit de considérer $-x = p_0, \alpha_1 \ldots \alpha_n \ldots \geqslant 0$.

Exemples :

$$\begin{aligned} 27{,}482\,999 \ldots &= 27{,}483 \\ &= 27{,}483\,000 \ldots \\ -\,4{,}395\,799 \ldots &= -\,(4{,}395\,8) \\ &= -\,4{,}395\,800\,0 \ldots \end{aligned}$$

Les deux cas ne pouvant se présenter que pour les nombres décimaux nous pouvons conclure

Théorème.

Pour tout nombre réel non décimal x, il existe un développement décimal illimité unique égal à x.

Pour tout décimal $x = A\,10^{-k}$ $(A \in \mathbb{Z}, k \in \mathbb{N})$ il existe deux développements décimaux illimités égaux à x :

l'un, développement décimal illimité propre, a toutes ses décimales d'ordre $> k$ égales à 0;

l'autre, développement décimal illimité impropre, a toutes ses décimales d'ordre $> k$ égales à 9.

REMARQUES

4. On dit qu'une suite infinie réelle (u_n) est *périodique* s'il existe un entier naturel k et un entier naturel h tel que

   pour tout $n > k$ $\quad u_{n+h} = u_n$.

   On dit que le *développement décimal illimité* $p_0, \alpha_1, \ldots \alpha_n \ldots$ est *périodique* si la suite (α_n) est périodique. Par exemple pour

   $$21,\ 73\ 152\ 152\ 152 \ldots . \qquad (k = 2 \quad h = 3)$$

   152 est la *période* et 21,73 la *partie irrégulière*.

   Pour un développement décimal illimité propre d'un décimal, $h = 1$, et la période est 0; pour le développement impropre on a aussi $h = 1$ mais la période est 9.

   On démontre $x = p, \alpha_1 \ldots, \alpha_n \ldots$ est périodique si et seulement si x est *rationnel* (cf. exercice 3.77 à la fin du chapitre).

5. Soit a un entier naturel supérieur à 2. Tout ce que nous avons dit en base 10 peut se transposer en base a.

Les nombres réels de la forme A a^{-k} ($A \in \mathbb{Z}$ et $k \in \mathbb{N}$) jouent le rôle des nombres décimaux. Ce sont les rationnels dont la représentation irréductible p/q est telle que les seuls facteurs premiers de q sont des facteurs premiers de la base a. Ces nombres s'écrivent en base a

$$\varepsilon\left(p_0 + \frac{\alpha_1}{a} + \ldots + \frac{\alpha_n}{a^n}\right) = \varepsilon\, p_0, \alpha_1 \ldots \alpha_n$$

où $\varepsilon = +1$ ou -1, $p_0 \in \mathbb{N}$ et

$$(\forall n \in \mathbb{N}^*) \qquad \alpha_n \in \{0, 1, 2, \ldots, a-1\}$$

On pourra dire que ces nombres sont les nombres à virgule en base a et que α_k est chiffre de rang k, après la virgule. On pourra étudier de même les développements illimités en base a. Un réel x admettra un développement illimité unique en base a si et seulement si a n'est pas de la forme Aa^{-k} ($A \in \mathbb{Z}$, $k \in \mathbb{N}$).

3. 22 VALEURS APPROCHÉES. ERREUR. INCERTITUDE. ENCADREMENT

a) Introduction.

Sauf lorsqu'il s'agit de nombres rationnels « simples », c'est-à-dire de quotients entiers dont la valeur absolue est inférieure à 100, ou même à 10, les calculs pratiques, lorsqu'ils sont effectués à la main, avec ou sans table de logarithmes, à la règle à calcul, ou avec certaines machines à calcul dites de bureau, utilisent la représentation décimale des nombres réels. Les calculatrices électroniques travaillent avec le système binaire, mais le plus souvent reçoivent les données et fournissent les résultats dans le système décimal.

C'est dire que dans un calcul pratique, un nombre réel non décimal n'interviendra jamais par sa valeur exacte, mais seulement par des valeurs décimales plus ou moins proches de cette valeur exacte.

b) Erreur, incertitude.

Lorsqu'on remplace un nombre réel x par un nombre x' on commet une *erreur* $x' - x = e$. Si $e < 0$ on dit que x' est une *valeur approchée* de x par *défaut;* si $e > 0$ on dit que x' est une *valeur approchée* par *excès*.

En général x' est le résultat d'une mesure ou le résultat approché d'un calcul précédent et on ne connaît pas l'erreur, sinon on connaîtrait $x = x' + e$ exactement. Mais dans la plupart des cas on connaît un *majorant* de $|e|$ (c'est-à-dire un majorant de l'ensemble des valeurs $|e|$).

Ce majorant ε de $|e|$ est appelé l'**incertitude** avec laquelle on connaît le nombre x lorsque l'on prend x' pour valeur approchée de x.

On a donc

$$|x' - x| = |e| < \varepsilon,$$

c'est-à-dire

$$x' - \varepsilon < x < x' + \varepsilon.$$

On dit que x est *encadré* par $x' - \varepsilon$ et $x' + \varepsilon$.

c) Encadrement.

D'une manière générale s'il existe deux nombres réels a et b tels que

$$a < x < b$$

on dit que x est **encadré** par a et b.

Le nombre a est une *valeur approchée par défaut, l'incertitude étant* $b - a$.
Le nombre b est une *valeur approchée par excès, l'incertitude étant encore* $b - a$.

Si l'on prend pour valeur approchée de x le nombre $x' = \frac{a+b}{2}$ *on ne connaît pas le sens de l'approximation,* x pouvant être soit dans $\left[a, \frac{a+b}{2}\right]$ soit dans $\left[\frac{a+b}{2}, b\right]$ l'incertitude, avec le choix de $x' = \frac{a+b}{2}$ pour valeur approchée de x, est $\frac{b-a}{2}$.

En posant $x' = \frac{a+b}{2}$ et $\varepsilon = \frac{b-a}{2}$ nous avons $a = x' - \varepsilon$ et $b = x' + \varepsilon$ et par conséquent

$$x' - \varepsilon < x < x' + \varepsilon.$$

Un résultat numérique x pourra s'exprimer de plusieurs manières équivalentes :
1° Par *encadrement* $a < x < b$.
Par exemple :

$$1{,}41421 < \sqrt{2} < 1{,}41422.$$

2° Par la donnée de *la plus petite valeur d'encadrement* a (valeur approchée par défaut) et l'*incertitude* ε; on a alors

$$a < x < a + \varepsilon.$$

3° Par la donnée de *la plus grande valeur d'encadrement* b (valeur approchée par excès et l'*incertitude* ε, on a alors

$$b - \varepsilon < x < b.$$

4° Par une valeur approchée x' et l'incertitude ε, on a alors

$$x' - \varepsilon < x < x' + \varepsilon.$$

Par exemple 1,414215 est une valeur approchée de $\sqrt{2}$, l'incertitude est 5.10^{-6}.

d) Conclusion.

Dans la pratique, a et b seront des nombres décimaux. On sait que si x est un réel donné, il existe pour tout entier positif n, un nombre décimal unique de la forme $p_n.10^{-n}$, où $p_n \in \mathbb{Z}$ tel que

$$p_n.10^{-n} \leqslant x < (p_n + 1).10^{-n}$$

On peut donc *théoriquement* encadrer un nombre réel par des décimaux avec une incertitude aussi petite que l'on veut.
Pratiquement, on est cependant limité :
— soit par la dimension des calculatrices. Pour chacune d'elles, le nombre des décimales qu'elle peut enregistrer est limité :
— soit par la précision des tables de logarithmes (les plus usuelles sont « à quatre ou à cinq décimales »), ou de la règle à calcul;
— soit par le temps rapidement croissant que demande une plus grande précision.
N'oublions pas enfin que beaucoup de données numériques ont une origine expérimentale, et à ce titre ne peuvent être fournies qu'avec une incertitude qui dépend de la précision des instruments de mesure et du soin de l'expérimentation, mais qui de toute manière ne pourra pas descendre au-dessous d'une certaine valeur.

En conclusion, tout calcul pratique sera effectué sur des valeurs approchées décimales.

REMARQUE

Si $x = p_0, \alpha_1 \ldots \alpha_n \alpha_{n+1} \ldots$ le décimal $a_n = p_0, \alpha_1 \ldots \alpha_n$ est la valeur approchée par défaut à 10^{-n} près, c'est-à-dire l'incertitude est 10^{-n}.
On fait souvent la convention suivante :
si $\alpha_{n+1} < 5$ on prend pour valeur approchée $x' = a_n$
si $\alpha_{n+1} \geqslant 5$ — — $x' = a_n + 10^{-n}$
(on dit dans ce cas que l'on « force » la $n^{\text{ième}}$ décimale). En prenant ainsi x' pour valeur approchée de x l'incertitude n'est plus que $\frac{1}{2}10^{-n} = 5 \times 10^{-(n+1)}$ *mais on ne connaît pas le sens de l'approximation.*

3. 23 REMARQUES GÉNÉRALES SUR LES CALCULS APPROCHÉS

a) Ordre de grandeur. Chiffres significatifs.

Une présentation commode d'un résultat numérique consiste à l'écrire sous la forme d'un nombre compris entre 1 et 10 multiplié par une puissance (positive ou négative) de 10.

Par exemple 371,43 s'écrira $3{,}7143 \times 10^2$
0,0000421 s'écrira $4{,}21 \times 10^{-5}$

Ainsi tout décimal x peut s'écrire sous la forme

$$x = d\,10^p \quad \text{avec} \quad 1 \leqslant |d| < 10 \quad \text{et} \quad p \in \mathbb{Z}.$$

cette écriture de x est appelée *écriture normalisée* du décimal x.
L'exposant p de 10 fournit un premier encadrement puisque sa donnée permet d'affirmer que $10^p \leqslant |x| < 10^{p+1}$. Elle donne une première idée de l'ordre de grandeur de x, et toute faute de calcul sur p dénature le résultat et est *la plus grave des fautes que l'on puisse commettre.*
La précision avec laquelle doit être donnée une valeur approchée dépend de ce que l'on sait de l'incertitude avec laquelle elle permet d'encadrer la valeur exacte.
Supposant par exemple que la terre est assimilable à une sphère, cherchons son rayon en kilomètres en prenant pour valeur approchée par défaut de π le nombre 3,14 avec une incertitude de 10^{-2}.
Si l'on « calcule » $\frac{20\,000}{3{,}14}$, on peut donner autant de décimales que l'on veut, et en donner une valeur approchée telle que la suivante 6369,4. *Or, dans les conditions où l'on s'est placé les deux derniers chiffres n'ont aucune valeur.* On veut en effet évaluer $\frac{20\,000}{\pi}$ avec $3{,}14 < \pi < 3{,}15$. On a donc

$$\frac{20\,000}{3{,}15} < \frac{20\,000}{\pi} < \frac{20\,000}{3{,}14}.$$

Or une valeur approchée par défaut de $\frac{20\,000}{3{,}15}$ est 6349,2 et une valeur approchée par excès de $\frac{20\,000}{3{,}14}$ est 6369,5.
Tout ce que l'on peut affirmer est donc que l'on a pour le rayon R de la terre exprimé en kilomètres

$$6349{,}2 < R < 6369{,}5$$

On peut donner le résultat sous la forme $6{,}36.10^3$ qui est une valeur approchée de R avec une erreur inférieure à 11 km.
(Sachant d'ailleurs que π est plus proche de 3,14 que de 3,15, on peut affirmer, sans faire le calcul avec une valeur approchée plus précise de π, que l'erreur est certainement inférieure à 10 km, et que $6{,}36.10^3$ est très vraisemblablement une valeur approchée par défaut.)
Il est certain, en tout cas, que donner le résultat sous la forme 6349,2 ou 6369,5 n'est pas recommandable puisque l'on a lieu de penser que les derniers chiffres écrits n'apportent aucune information valable. Par contre ceux de $6{,}36.10^3$, que l'on qualifie souvent de chiffres significatifs, donnent ce que l'on connaît du nombre R : le premier 6 et le 3 sont certainement exacts; dans une valeur plus approchée de R, le second 6 risque d'être remplacé par un 5.

EXERCICE

Refaire ces calculs avec $3{,}1415 < \pi < 3{,}1416$.

b) Erreur et incertitude relatives.

Lorsque l'on mesure une longueur l à 1 mm près, la précision n'est pas la même selon que l'on mesure une page de cahier ou une table. Cette remarque nous conduit aux définitions suivantes :

Soit x' une valeur approchée de x, $e = x' - x$ l'erreur et ε l'incertitude, le nombre $\frac{e}{x}$ est appelé *erreur relative* ou *taux d'erreur* et le nombre $\frac{\varepsilon}{|x|}$ incertitude *relative* ou *taux d'incertitude*. Pratiquement on remplacera $|x|$ par un minorant de $|x|$.

3. 24 OPÉRATIONS SUR DES VALEURS APPROCHÉES

a) Incertitude sur une somme.

Soient deux nombres réels x et y connus chacun par un encadrement. On a

$$a < x < a + h, \quad b < y < b + k.$$

d'où $a + b < x + y < a + b + h + k$; $a + b$ est donc une valeur approchée de $x + y$ et l'incertitude sur $x + y$ est $h + k$, somme des incertitudes sur x et sur y.
Remarquons qu'à tout encadrement $a < x < a + h$ correspond un encadrement de $-x$, on a, en effet, $-(a + h) < -x < -a$ pour lequel l'incertitude est la même.
On peut donc conclure :

> L'incertitude sur une somme de nombres réels ou de leurs opposés est la somme des incertitudes associées à chacun d'eux.

Il y a donc une perte de précision.

b) Incertitude sur un produit.

Soient x et y deux nombres réels *positifs*, encadrés par des nombres réels *positifs*

$$a < x < a + h, \quad b < y < b + k.$$

On en déduit $ab < xy < ab + bh + ak + hk$.

ab est une valeur approchée par défaut, et l'incertitude est $bh + ak + hk$; elle dépend non seulement des incertitudes sur x et y, mais des valeurs approchées a et b.

Il est commode à ce propos d'écrire les encadrements sous la forme

$$a < x < a(1 + \varepsilon), \quad b < y < b(1 + \eta)$$

où $\varepsilon = \dfrac{h}{a}$ et $\eta = \dfrac{k}{b}$ sont les *incertitudes relatives sur x et y*; elles seront toujours pratiquement entre 0 et 1. Dans ces conditions, on a

$$ab < xy < ab(1 + \varepsilon + \eta + \eta\varepsilon).$$

L'incertitude relative sur le produit est $\varepsilon + \eta + \varepsilon\eta$. Dans la pratique, ε et η sont « petits » et $\varepsilon\eta$ est « négligeable ». Par exemple, si $\varepsilon = \eta = 10^{-3}$ on a $\varepsilon\eta = 10^{-6}$, et il est raisonnable de considérer que l'incertitude relative sur le produit est alors 2.10^{-3}.

Dans la pratique l'incertitude relative sur un produit de nombres positifs est la somme des incertitudes relatives sur chacun des facteurs.

Soit l l'incertitude sur xy; l'incertitude relative est $\dfrac{l}{xy}$; on a donc $\dfrac{l}{xy} = \varepsilon + \eta$; dans la pratique on peut confondre $\dfrac{h}{a}$ et $\dfrac{h}{x}$ et de même $\dfrac{k}{b}$ et $\dfrac{k}{y}$ d'où

$$l = (\varepsilon + \eta)\,xy = \left(\frac{h}{x} + \frac{k}{y}\right)xy = hy + kx.$$

REMARQUE

1. Si x et y ne sont pas tous deux positifs, on applique les considérations précédentes aux valeurs absolues de x, y et xy.

c) Incertitude sur l'inverse.

Supposons x positif, encadré par a et $a + h$ avec $0 < a$. Posons $a + h = a(1 + \varepsilon)$. On a $a < x < a(1 + \varepsilon)$, on en déduit $\dfrac{1}{a(1 + \varepsilon)} < \dfrac{1}{x} < \dfrac{1}{a}$. Mais on peut remarquer que $1 - \varepsilon < \dfrac{1}{1 + \varepsilon}$ (car $1 - \varepsilon^2 < 1$), et que l'on peut écrire

$$\frac{1}{a}(1 - \varepsilon) < \frac{1}{x} < \frac{1}{a}$$

ou encore, en posant $b = \dfrac{1}{a(1 + \varepsilon)}$, $\quad b < \dfrac{1}{x} < b(1 + \varepsilon)$.

Ce qui prouve que l'*incertitude relative sur* $\dfrac{1}{x}$ *est la même que l'incertitude sur x.*

Soit m l'incertitude sur $\dfrac{1}{x}$, en confondant toujours $\dfrac{h}{a}$ et $\dfrac{h}{x}$ on a

$$\frac{m}{\left(\frac{1}{x}\right)} = \varepsilon = \frac{h}{x}$$

d'où $\qquad m = \dfrac{h}{x^2}.$

REMARQUE

2. Le résultat précédent concerne l'incertitude relative. Il faut noter que si x est voisin de 0, l'incertitude sur $\frac{1}{x}$ peut être considérable. Si l'on sait que $10^{-6} < x < 2.10^{-6}$, $\frac{1}{x}$, lui, est compris entre 5.10^5 et 10^6.

Les résultats précédents montrent que l'incertitude relative sur $\frac{x}{y}$ ($x > 0$ et $y > 0$) est la somme des incertitudes relatives sur x et sur y.

EXERCICE

On pose $0 < a < x < a + h$, $0 < b < y < b + k$ $h = a\varepsilon$, $k = b\eta$. Calculer en fonction de x, y, h, k l'incertitude sur $\frac{x}{y}$.

3. 25 VALEURS APPROCHÉES USUELLES

Nous nous proposons de trouver des valeurs approchées des nombres $(1 + x)^2$, $\sqrt{1 + x}$, $\frac{1}{1 + x}$, $\frac{1}{\sqrt{1 + x}}$ de la forme $1 + kx$, k étant un nombre réel ne dépendant pas de x, lorsque $|x|$ est « petit ». Non précisée, la dernière locution n'a pas de sens; c'est pour cela que nous avons mis le mot « petit » entre guillemets; dans certaines situations, on aura $|x| < \frac{1}{10}$, dans d'autres $|x| < \frac{1}{1\,000}$ etc. En tout état de cause nous supposerons toujours que $|x| < \frac{1}{2}$; dans ce cas l'erreur commise dans les approximations que nous allons faire est toujours inférieure à $2x^2$; nous le démontrerons dans certains cas, nous l'admettrons dans les autres cas.

a) Valeurs approchées de $(1 + x)^2$ et $\sqrt{1 + x}$.

Nous avons

$$(1 + x)^2 = 1 + 2x + x^2.$$

Le nombre $1 + 2x$ est une valeur approchée par *défaut* de $(1 + x)^2$, l'erreur est x^2. Si $|x| < \frac{1}{10}$ l'erreur est inférieure à $\frac{1}{100}$, si $|x| < \frac{1}{100}$ l'erreur est inférieure à $\frac{1}{10\,000}$, etc.

Nous dirons dans ces conditions que les nombres $(1 + x)^2$ et $1 + 2x$ sont peu différents; nous écrirons

$$\boxed{(1 + x)^2 \simeq 1 + 2x}$$

qui se lit : « $(1 + x)^2$ *est peu différent de* $1 + 2x$ ».

Nous pouvons penser que si les deux nombres *positifs* $1 + 2y$ et $(1 + y)^2$ sont peu différents alors il en est de même de $\sqrt{1 + 2y}$ et $1 + y$. En posant $2y = x$ nous aurons

$$\boxed{\sqrt{1 + x} \simeq 1 + \frac{x}{2}}$$

Le nombre $1 + \frac{x}{2}$ est une valeur approchée par *excès* de $\sqrt{1+x}$, en effet on a

$$1 + x < 1 + x + \frac{x^2}{4} = \left(1 + \frac{x}{2}\right)^2.$$

EXERCICE

1. On pose

$$1 + \frac{x}{2} = \sqrt{1+x} + e$$

($e > 0$); montrer que e est racine du trinôme f défini pour tout nombre réel u par

$$f(u) = u^2 - (x+2)\,u + \frac{x^2}{4}.$$

Calculer $f\left(\frac{x^2}{8}\right)$ et $f(2)$. En déduire que pour x *positif* on a $e < \frac{x^2}{8}$.

Nous admettrons que pour x négatif tel que $|x| < \frac{1}{2}$ on a $e < \frac{x^2}{4}$.

b) Valeur approchée de $\frac{1}{1+x}$.

Nous avons

$$1 - x^2 = (1-x)(1+x)$$

ou encore

$$1 = (1-x)(1+x) + x^2$$

d'où

$$\frac{1}{1+x} = 1 - x + \frac{x^2}{1+x}.$$

Le nombre $1 - x$ est donc une valeur approchée par *défaut* de $\frac{1}{1+x}$; l'erreur est $\frac{x^2}{1+x}$; si x est positif cette erreur est inférieure à x^2; si x est négatif et tel que $|x| < \frac{1}{2}$ cette erreur est inférieure à $2x^2$. Nous écrirons

$$\boxed{\frac{1}{1+x} \simeq 1 - x.}$$

c) Valeur approchée de $\frac{1}{\sqrt{1+x}}$.

Le nombre $1 + \frac{x}{2}$ est peu différent de $\sqrt{1+x}$, nous pouvons penser que $\frac{1}{\sqrt{1+x}}$ est peu différent de $\frac{1}{1+\frac{x}{2}}$ qui est peu différent de $1 - \frac{x}{2}$. Nous admettrons que l'on a

$$\boxed{\frac{1}{\sqrt{1+x}} \simeq 1 - \frac{x}{2}}$$

et que l'erreur est inférieure à $\frac{3x^2}{8}$ si x est positif et à $\frac{3x^2}{4}$ si $-\frac{1}{2} < x < 0$.

EXERCICE

2. Démontrer que $1 - \frac{x}{2}$ est une valeur approchée par défaut de $\frac{1}{\sqrt{1+x}}$.

d) Conclusion.

Nous voyons que si pour tout nombre réel $a > 0$ on pose

$$\frac{1}{\sqrt{a}} = \frac{1}{a^{\frac{1}{2}}} = a^{-\frac{1}{2}}$$

nous aurons pour $|x|$ « petit » et pour $\alpha \in \left\{2, -2, -1, \frac{1}{2}, -\frac{1}{2}\right\}$

$$\boxed{(1+x)^{\alpha} \simeq 1 + \alpha x.}$$

D'autre part nous avons vu que si $|x| < \frac{1}{2}$ l'erreur commise en remplaçant $(1+x)^{\alpha}$ par $1 + \alpha x$ est inférieure dans tous les cas étudiés à $2x^2$.

EXEMPLES

1. $\sqrt{97} = \sqrt{100 - 3} = 10\sqrt{1 - 3.10^{-2}} \simeq 10\,(1 - 1{,}5.10^{-2}) = 10 - 0{,}15 = 9{,}85.$

2. $\frac{1}{\sqrt{10016}} = \frac{1}{100\sqrt{1 + 16.10^{-4}}} \simeq 10^{-2}\,(1 - 8.10^{-4}) = 10^{-2} - 8.10^{-6} = 0{,}009992.$

EXERCICES

Calculs dans le corps totalement ordonné $\mathbb{R}$: 1 à 12, 17 à 19.
Nombres rationnels : 13, 22 à 24, 77.
Partie entière : 14 à 16.
Formule du binôme : 20-21, 27, 38, 56.
Homomorphismes, isomorphismes : 25 à 27, 76.
Bornes supérieures, inférieures : 28, 29, 42.
Suites arithmétiques et géométriques : 30 à 34.
Limite d'une suite infinie : 33 à 58.
Calculs numériques : 44, 45, 51, 59 à 75, 77.

3.1 Soit x et y deux nombres réels strictement positifs; comparer les nombres a, $g > 0$ et h définis respectivement par

$$2a = x + y \quad , \quad g^2 = xy \quad , \quad \frac{2}{h} = \frac{1}{x} + \frac{1}{y}.$$

3.2 Démontrer que, quels que soient le réel $x > 0$, on a $x + \frac{1}{x} \geqslant 2$.

Application : Quels que soient les réels $a > 0$ et $b > 0$, on a $\frac{a}{b} + \frac{b}{a} \geqslant 2$.

3.3 Soit (a_n) une suite infinie de nombres réels strictement positifs définie pour $n \geqslant 1$; on considère la suite (x_n) définie pour tout $n \geqslant 1$ par

$$x_n = (a_1 + \ldots + a_n)\left(\frac{1}{a_1} + \ldots + \frac{1}{a_n}\right).$$

Soit $\mathfrak{T}$ la propriété définie, pour tout $n \geqslant 1$, par $x_n \geqslant n^2$.
a) Démontrer $\mathfrak{T}(1)$.
b) Démontrer que pour tout $n \geqslant 1$ $\quad \mathfrak{T}(n) \Longrightarrow \mathfrak{T}(n+1)$.
(On écrira $x_{n+1} = x_n + a_{n+1}\left(\frac{1}{a_1} + \ldots + \frac{1}{a_n}\right) + (a_1 + \ldots + a_n)\frac{1}{a_{n+1}} + 1$ et on utilisera l'ex. 3.2.)
c) Conclure pour tout $n \geqslant 1$ on a $x_n \geqslant n^2$. Dans quel cas a-t-on $x_n = n^2$?

3.4 Soit a et b deux nombres réels tels que pour tout x de $]b, +\infty[$ on ait $a \leqslant x$. Démontrer que $a \leqslant b$.

3.5 Démontrer que, quels que soient les réels x, y, x', y', on a

$$(x^2 + y^2)(x'^2 + y'^2) = (xx' + yy')^2 + (xy' - yx')^2.$$

Donner une interprétation géométrique à l'aide des vecteurs $\vec{V}(x, y)$ et $\vec{V}'(x', y')$ du plan vectoriel euclidien.

3.6 Démontrer que, quels que soient les réels x, y, z, x', y', z', on a
$(x^2 + y^2 + z^2)(x'^2 + y'^2 + z'^2)$
$= (xx' + yy' + zz')^2 + (yz' - zy')^2 + (zx' - xz')^2 + (xy' - yx')^2$

Vous verrez en géométrie une interprétation de cette formule à l'aide des vecteurs $\vec{V}(x, y, z)$ et $\vec{V}'(x', y', z')$ de $\mathcal{E}_3$.

3.7* *a*) Développer $(x + y + z)(-x + y + z)(x - y + z)(x + y - z)$ où x, y, z sont des nombres réels quelconques.

b) Calculer $(r + r' + 2a)(-r + r' + 2a)(r - r' + 2a)(r + r' - 2a)$ avec

$$r = \sqrt{(x-c)^2 + y^2} \quad , \quad r' = \sqrt{(x+c)^2 + y^2},$$

où x, y, a, c sont des réels quelconques.

c) Dans le plan euclidien E_2, on considère les points $M(x, y)$, $F(c, 0)$, $F'(-c, 0)$.

α) On suppose $0 < c < a$ et on pose $b^2 = a^2 - c^2$; démontrer que, quel que soit M, on a

$$(MF + MF' = 2a) \iff \left(\frac{x^2}{a^2} + \frac{y^2}{b^2} - 1 = 0\right).$$

β) On suppose $0 < a < c$ et on pose $b^2 = c^2 - a^2$; démontrer que, quel que soit M, on a

$$(|MF - MF'| = 2a) \iff \left(\frac{x^2}{a^2} - \frac{y^2}{b^2} - 1 = 0\right).$$

3.8 Calculer, quels que soient les réels x, y, z, $(x + y + z)^2$ et $(x + y + z)^3$.

3.9 Démontrer que, quels que soient les réels x, y, z, on a

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - yz - zx - xy)$$
$$= \frac{(x + y + z)}{2}[(y - z)^2 + (z - x)^2 + (x - y)^2].$$

Application : Trouver les solutions réelles de l'équation en x

$$x^3 - 3abx + a^3 + b^3 = 0$$

où a et b sont des réels quelconques donnés.

3.10 Soit trois nombres réels strictement positifs. Comparer $\frac{x}{y}$ et $\frac{x+z}{y+z}$.

3.11 Soit $(a_i)_{1 \leqslant i \leqslant n}$ et $(a'_i)_{1 \leqslant i \leqslant n}$ deux suites finies de nombres réels ($a'_i \neq 0$ pour tout i de $[1, n]$ et $a'_1 + a'_2 + \ldots + a'_n \neq 0$); démontrer par récurrence que

$$\left(\frac{a_1}{a'_1} \leqslant \ldots \leqslant \frac{a_i}{a'_i} \leqslant \ldots \leqslant \frac{a_n}{a'_n}\right) \Longrightarrow \left(\frac{a_1}{a'_1} \leqslant \frac{a_1 + \ldots + a_n}{a'_1 + \ldots + a'_n} \leqslant \frac{a_n}{a'_n}\right).$$

3.12 Soit $(x_i)_{1 \leqslant i \leqslant n}$ une suite finie de nombres réels non nuls; k étant un réel non nul on pose $y_i = kx_i$ ($1 \leqslant i \leqslant n$). Démontrer que, quel que soit l'entier naturel p et la suite $(x_i)_{1 \leqslant i \leqslant n}$ de nombres réels tels que $\alpha_1 x_1^p + \ldots + \alpha_n x_n^p \neq 0$, la valeur du nombre

$$\frac{\alpha_1 y_1^p + \ldots + \alpha_n y_n^p}{\alpha_1 x_1^p + \ldots + \alpha_n x_n^p}$$

est indépendante du choix de la suite finie (α_i).

3.13 *a*) Démontrer que si x est irrationnel et a rationnel, alors $x + a$ et ax sont irrationnels.

b) Les nombres a, b, c, d étant rationnels et x irrationnel le nombre $\frac{ax + b}{cx + d}$ (où on suppose $cx + d \neq 0$) est-il rationnel ou irrationnel?

3.14 On note $[x]$ la partie entière du réel x, c'est-à-dire $[x]$ est l'entier relatif n tel que $n \leqslant x < n + 1$. Démontrer que l'on a

$$[x + y] = [x] + [y] + \varepsilon \quad \text{avec} \quad \varepsilon = 0 \quad \text{ou} \quad \varepsilon = 1,$$
$$[x - y] = [x] - [y] - \varepsilon \quad \text{avec} \quad \varepsilon = 0 \quad \text{ou} \quad \varepsilon = 1.$$

3.15* Démontrer que, quel que soit l'entier $p \geqslant 1$ on a

$$[x] + \left[x + \frac{1}{p}\right] + \ldots + \left[x + \frac{p-1}{p}\right] = [px].$$

3.16 Démontrer que, quel que soit l'entier $p \geqslant 1$ on a

$$\left[\frac{[px]}{p}\right] = [x].$$

3.17 *a*) Démontrer que, quels que soient les réels x et y, on a

$$\sup(x,y) = \frac{1}{2}[(x+y) + |x-y|] \quad , \quad \inf(x,y) = \frac{1}{2}[(x+y) - |x-y|].$$

b) On pose, pour tout x réel, $x^+ = \sup(x, 0)$ et $x^- = \sup(-x, 0)$. Calculer x^+ et x^- à l'aide de x et $|x|$.

3.18 Pour tout $x \neq 2$ on pose

$$f(x) = \sup\left(x^2 + 2x - 3 \ , \ \frac{x-1}{x-2} \ , \ x - 1\right).$$

Donner, suivant les valeurs de x, une expression de $f(x)$ à l'aide de x sans utiliser le symbole sup.

3.19 Soit $\mathfrak{T}(n)$ l'énoncé suivant : « Tout polynôme f à coefficients réels, de degré $\leqslant n$, écrit sous forme réduite et tel que

$$(\forall x \in \mathbb{R}) \qquad f(x) = 0$$

a tous ses coefficients nuls ».

a) Démontrer $\mathfrak{T}(1)$ et $\mathfrak{T}(0)$.

b) Démontrer que pour tout n de $\mathbb{N}$, $\mathfrak{T}(n)$ implique $\mathfrak{T}(n+1)$. (On considérera les polynômes f et g définis respectivement par

$$f(x) = a_0 + a_1 x + \ldots + a_{n+1}x^{n+1},$$
$$g(x) = f(2x) - 2^{n+1} f(x).$$

Conclure.

c) *Application :* Que peut-on dire des polynômes A et B définis, quel que soit x, par

$$A(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \text{et} \quad B(x) = b_0 + b_1 x + \ldots + b_n x^n$$

si, pour tout x de $\mathbb{R}$, on a $A(x) = B(x)$?

3.20 En utilisant la formule du binôme donnant $(1+x)^n$, calculer

a) $\sum_{p=0}^{p=n} C_n^p$ *b*) $\sum_{p=0}^{p=n} (-1)^p C_n^p$ *c*) $C_n^0 + C_n^2 + C_n^4 + \ldots$

d) $C_n^1 + C_n^3 + C_n^5 + \ldots$.

3.21 *a*) Démontrer que $\sum_{p=0}^{p=n} (C_n^p)^2 = C_{2n}^n$ (Calculer le terme en x^n dans $(1+x)^n (1+x)^n$ et dans $(1+x)^{2n}$ puis appliquer le résultat de l'exercice 3.19 c).

b) Déduire de la formule précédente que $\sum_{p=0}^{p=n} p\,(C_n^p)^2 = \frac{n}{2} C_{2n}^n$.

3.22 *a*) Démontrer que, quels que soient les nombres rationnels a, a', b, b', on a

$$(a + a'\sqrt{2} = 0) \Longrightarrow (a = a' = 0)$$
$$(a + a'\sqrt{2} = b + b'\sqrt{2}) \Longrightarrow (a = b \quad \text{et} \quad a' = b').$$

b) Ces résultats subsistent-ils si on remplace $\sqrt{2}$ par un nombre irrationnel quelconque?

3.23 Démontrer que quels que soient les nombres rationnels a, a', a'', on a

$$(a\sqrt{2} + a'\sqrt{3} + a''\sqrt{5} = 0) \Longrightarrow (a = a' = a'' = 0).$$

3.24* On pose $\omega = \sqrt[3]{2}$ et on considère trois nombres rationnels α, β, γ tels que $\alpha + \beta\omega + \gamma\omega^2 = 0$.

a) Démontrer que si l'un des nombres α, β, γ est nul, les deux autres le sont.

b) Démontrer qu'il existe a et b rationnels tels que $a + b\omega = 0$ (remarquer que l'on a aussi $\alpha\omega + \beta\omega^2 + 2\gamma = 0$).

c) Démontrer que, quels que soient α, β, γ rationnels, on a

$$(\alpha + \beta\omega + \gamma\omega^2 = 0) \Longrightarrow (\alpha = \beta = \gamma = 0).$$

3.25 *a*) Démontrer que l'ensemble E des nombres réels de la forme $a + a'\sqrt{2}$ où a et a' sont deux rationnels quelconques est un sous-corps de $\mathbb{R}$; il se note $\mathbb{Q}[\sqrt{2}]$.

b) On désigne par E' l'ensemble $\mathbb{Q} \times \mathbb{Q}$ muni des lois internes suivantes :

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a')(b, b') = (ab + 2a'b', ab' + ba')$$

Démontrer que l'application

$$f : \mathrm{E} \longrightarrow \mathrm{E}'$$
$$a + a'\sqrt{2} \longmapsto (a, a')$$

définit un isomorphisme de $(\mathrm{E}, +, \times)$ sur $(\mathrm{E}', +, \times)$.

3.26* On considère un homomorphisme φ du corps $\mathbb{Q}[\sqrt{2}]$ dans lui-même (cf. ex. 2.25).

a) Démontrer que, s'il existe $a + a'\sqrt{2} \neq 0$ tel que $\varphi(a + a'\sqrt{2}) \neq 0$, alors $\varphi(1) = 1$. En déduire que, dans ce cas, pour tout rationnel a, on a $\varphi(a) = a$. (On commencera par montrer que pour tout n de $\mathbb{N}$ on a $\varphi(n) = n$).

b) Quelle est la valeur de $[\varphi(\sqrt{2})]^2$?

c) Démontrer que les seuls homomorphismes φ distincts de l'application nulle sont l'application identique et l'isomorphisme $a + a'\sqrt{2} \longmapsto a - a'\sqrt{2}$.

3.27 On désigne par D l'ensemble $\mathbb{R} \times \mathbb{R}$ muni des lois internes suivantes :

$$(a, a') + (b, b') = (a + b, a' + b'),$$
$$(a, a')(b, b') = (ab, ab' + a'b).$$

a) Démontrer que $(\mathrm{D}, +, \times)$ est un anneau commutatif unitaire.

b) Démontrer que cet anneau possède de véritables diviseurs de zéro.

c) On désigne par D' l'ensemble des éléments de D de la forme (a, 0). Démontrer que D' est stable pour l'addition et la multiplication et que l'application

$$\varphi : \mathbb{R} \longrightarrow \mathrm{D}'$$
$$a \longmapsto (a, 0)$$

définit un isomorphisme de $(\mathbb{R}, +, \times)$ sur $(\mathrm{D}', +, \times)$. On identifiera a de $\mathbb{R}$ et $(a, 0)$ de D; donc $\mathbb{R} \subset \mathrm{D}$.

d) Grâce à l'identification précédente calculer, quels que soient α, a, a' réels, $\alpha(a, a')$. Démontrer que tout élément (a, a') de D s'écrit d'une manière unique $a + a'\varepsilon$ où $\varepsilon = (0, 1)$. Calculer ε^2.

e) Quels sont les éléments de D inversibles? Les éléments (a, a') et (b, b') étant donnés trouver (x, x') tels que $(a, a')(x, x') = (b, b')$, discuter.

f) Pour tout entier naturel $n \geqslant 2$ calculer $(x + y\varepsilon)^n$. Les nombres réels a et b étant donnés, chercher les réels x et y tels que $(x + y\varepsilon)^n = a + b\varepsilon$ (on étudiera d'abord le cas $n = 2$).

3.28 On désigne par V l'ensemble des valeurs d'une suite infinie (u_n) de nombres réels.
Déterminer, pour les suites suivantes, si V est majoré (resp. minoré), si sup V (resp. inf V) existe, si sup V (resp. inf V) appartient à V :

1° Pour tout n $\quad u_n = a + bn \qquad (a \in \mathbb{R}, b \in \mathbb{R}_+)$.

2° Pour tout n $\quad u_n = a + b(-1)^n \qquad (a \in \mathbb{R}, b \in \mathbb{R}_+)$.

3.29 Mêmes questions qu'à l'exercice 3.28 pour les suites

1° Pour tout $n \geqslant 1$ $\quad u_n = a + \dfrac{b}{n}$ (a et b strictement positifs).

2° Pour tout $n \geqslant 1$ $\quad u_n = a(-1)^n + \dfrac{b}{n}$ (a et b strictement positifs).

3° Pour tout $n \geqslant 1$ $\quad u_n = a + \dfrac{b}{n}(-1)^n$ (a et b strictement positifs).

3.30 *a*) Trouver trois termes consécutifs a, b, c d'une suite arithmétique connaissant $s = a + b + c$ et $p = abc$. Discuter. (On posera $a = x - r$, $b = x$, $c = x + r$).

Application numérique : $s = -9$, $p = 48$.

b) Trouver trois termes consécutifs a, b, c d'une suite géométrique connaissant $s = a + b + c$ et $p = abc$. Discuter. (On posera $a = xq^{-1}$, $b = x$, $c = xq$).

Application numérique : $p = -216$, $s = 14$.

3.31 Trouver n termes consécutifs d'une suite arithmétique de raison r donnée connaissant la somme s de ces n termes.

3.32 Soit (u_n) une suite géométrique de raison q. Calculer le produit $u_0u_1 \dots u_n$ en fonction de u_0, q et n. (On pourra utiliser le fait que u_ku_{n-k} $(0 \leqslant k \leqslant n)$ est indépendant de k).

3.33 Soit (u_n) la suite géométrique définie par $u_0 = 18$ et $u_3 = \frac{2}{3}$. On pose $s_n = u_0 + u_1 + \dots + u_n$; trouver la limite de (s_n) lorsque n tend vers $+\infty$.

3.34 Soit a un entier $\geqslant 2$ et α et β des entiers vérifiant $1 \leqslant \alpha \leqslant a - 1$ et $1 \leqslant \beta \leqslant a - 1$. Trouver les nombres x, y, z représenté en base a par

$$x = 0{,}\alpha\alpha\alpha\alpha\alpha\alpha \dots \quad ; \quad y = 0{,}\alpha0\alpha0\alpha0 \dots \quad ; \quad z = 0{,}\alpha\beta\alpha\beta\alpha\beta \dots$$

Applications numériques

1° $a = 2$, $\alpha = 1$; calculer x et y.
2° $a = 12$, $\alpha = 11$, $\beta = 2$; calculer x, y et z.

Etudier si les suites suivantes ont une limite l ou tendent vers $+\infty$ ou $-\infty$ lorsque n tend vers $+\infty$. On donne le terme général (ex. 35 à 37).

3.35 *a*) $u_n = \dfrac{5n - 1}{2n + 3}$. *b*) $u_n = \dfrac{5n + 7}{n^2 - n + 1}$.

c) $\dfrac{an^2 + bn + c}{n + 1}$ (discuter suivant les valeurs des réels a, b, c).

3.36 *a*) $u_n = \dfrac{2n + (-1)^n}{3n + (-1)^{n+1}}$ $(n \geqslant 1)$. *b*) $u_n = \dfrac{n^2 + \cos n}{3(n + 1)^2 \sin 5n}$.

c) $\dfrac{\sqrt{4n^2 + 3n + 1}}{5n - 6}$ $(n \geqslant 1)$.

3.37 *a*) $u_n = \dfrac{2^n - 3^n}{2^n + 3^n}$.

b) $u_n = \dfrac{a^n - b^n}{a^n + b^n}$ (discuter suivant la valeur relative des réels $a > 0$ et $b > 0$).

3.38 Soit a un réel tel que $a > 1$ et p un entier naturel tel que $p > 0$.
a) En posant $a = 1 + b$ démontrer que pour tout $n > p$ on a

$$a^n \geqslant \frac{n(n-1)\dots(n-p+1)}{p!} b^p.$$

b) En déduire que

$$\lim \frac{a^n}{n^p} = +\infty.$$

(On remarquera que $n(n-1)\dots(n-p+1)$ contient p facteurs.)

3.39 Soit a un réel strictement positif. Démontrer que

$$\lim \frac{n!}{a^n} = +\infty.$$

(Dans le cas où $a > 1$ on introduira la partie entière p de a et pour $n \geqslant p+1$ on écrira

$$\frac{n!}{a^n} = \frac{p!}{a^p} \frac{(p+1)(p+2)\ldots n}{a^{n-p}}\Big)$$

3.40 Étudier les suites définies pour tout entier naturel n par

1. $u_n = \dfrac{2^n + n^{10}}{3^n + n^{100}}$ 2. $u_n = \dfrac{25n^3 - 5^n}{n^{1000} + 5^n}$ (utiliser ex. 3.38).

(utiliser ex. 3.38).

3.41 Étudier les suites suivantes définies pour tout entier naturel n par

1. $u_n = \dfrac{1\,000^n + n!}{2^n + n!}$ (utiliser ex. 3.39).
2. $u_n = \dfrac{n! + n^{50}}{3n! + 100^n}$ (utiliser ex. 3.38 et 3.39).

3.42* *a*) Étudier suivant les valeurs de $x \in \mathbb{R} - \{-2\}$ la suite définie pour tout entier naturel n par

$$u_n = \frac{(1+x)^n - 1}{(1+x)^n + 1}.$$

Pour les valeurs de x où (u_n) a une limite on désignera celle-ci par $l(x)$.

b) Construire la courbe représentatrice de la fonction f définie pour tout $x \neq -2$ par

$$f(x) = (x^2 - 1)\, l(x).$$

c) On pose $E = f([-1, +1])$. Trouver les bornes supérieure et inférieure de E; ces bornes appartiennent-elles à E?

3.43 Soit a et b deux nombres réels. On définit la suite (u_n) par $u_1 = a + b$ et pour tout $n \geqslant 1$ par

$$u_{n+1} = a + b - \frac{ab}{u_n}.$$

a) Calculer, lorsque $a \neq b$, u_1, u_2, u_3 uniquement à l'aide de $a - b$, $a^2 - b^2$, $a^3 - b^3$, $a^4 - b^4$. Démontrer que le résultat obtenu est général ($a \neq b$).

b) Démontrer que la suite (u_n) a une limite, quels que soient a et b vérifiant $a \neq b$; trouver cette limite.

c) Calculer, lorsque $a = b$, u_1, u_2, u_3 en fonction de a. Démontrer que le résultat obtenu est général. Démontrer que, dans ce cas, $a = b$, (u_n) a une limite que l'on donnera.

3.44 On considère les deux suites (u_n) et (v_n) définies simultanément pour tout $n > 0$ par

$$u_n = 1 + \frac{1}{1!} + \ldots + \frac{1}{n!} \quad , \quad v_n = 1 + \frac{1}{1!} + \ldots + \frac{1}{n!} + \frac{1}{n.n!}.$$

a) Démontrer que ces deux suites sont des suites adjacentes. Leur limite commune est le nombre e qui joue un grand rôle en Analyse (cf. tome 2).

b) Démontrer que, pour tout $n > 0$, il existe un nombre réel unique θ_n vérifiant $0 < \theta_n < 1$ tel que

$$(1) \qquad e = 1 + \frac{1}{1!} + \ldots + \frac{1}{n!} + \frac{\theta_n}{n.n!}$$

c) Démontrer que e est irrationnel (on montrera que la formule précédente est impossible avec $e = \dfrac{m}{n}$ $(m \in \mathbb{N}, n \in \mathbb{N}^*)$.

d) Donner un encadrement décimal de e en faisant $n = 6$ dans la formule (1) (pour calculer la valeur décimale de $\dfrac{1}{n!}$ on remarquera qu'il suffit de diviser par n la valeur décimale de $\dfrac{1}{(n-1)!}$.

3.45 On donne un réel $a > 0$ et on considère la suite (u_n) définie par $u_0 > 0$ et, pour tout $n \geqslant 1$, par

$$u_n = \frac{1}{2}\left(u_{n-1} + \frac{a}{u_{n-1}}\right)$$

et la suite (v_n) définie, pour tout $n \geqslant 0$, par

$$v_n = \frac{u_n - \sqrt{a}}{u_n + \sqrt{a}}.$$

a) Calculer, pour tout $n > 0$, v_n en fonction de v_{n-1}. Discuter, suivant les valeurs de v_0, l'existence de la limite de la suite (v_n).

b) Démontrer que la suite (u_n) a pour limite $\sqrt{a}$.

c) On pose $u_n = \sqrt{a}\,(1 + \varepsilon_n)$. Calculer ε_{n+1} en fonction de ε_n.

Application numérique. On donne $a = 2$, $u_0 = 1{,}4$. Calculer les valeurs décimales de u_1, u_2, u_3. Donner à l'aide de u_3 un encadrement de $\sqrt{2}$ (on remarquera que pour $n \geqslant 1$ la suite est décroissante).

3.46* On considère la suite (u_n) définie par la donnée de u_o tel que $0 \leqslant u_0 \leqslant 2$ et pour tout $n > 0$ par

$$u_n = \sqrt{2 - u_{n-1}}.$$

On pose $p_n = u_{2n}$ et $q_n = u_{2n+1}$.

a) Démontrer que la suite (u_n) est bornée. Comparer p_n et q_n à 1.

b) Étudier le signe de $p_{n+1} - p_n$ et $q_{n+1} - q_n$ (on distinguera les cas $0 \leqslant u_0 < 1$ et $1 < u_0 \leqslant 2$).

c) Démontrer qu'il existe un entier p et un réel $A > 1$ tel que, pour tout $n > p$, on ait

$$|u_{n+1} - u_n| < \frac{|u_n - u_{n-1}|}{A}$$

$\left(\text{On remarquera que } \sqrt{a} - \sqrt{b} = \dfrac{a - b}{\sqrt{a} + \sqrt{b}}\right)$.

En déduire que $\lim (u_{n+1} - u_n) = 0$.

d) Conclure : la suite (u_n) a une limite que l'on déterminera.

3.47 Soit a et b deux nombres réels; on considère la suite (x_n) définie par la donnée de x_0 et, pour tout $n > 0$, par

$$x_n = ax_{n-1} + b.$$

a) Calculer x_n en fonction de a, b, x_0, n (on ajoutera membre à membre les égalités obtenues en multipliant $x_k = ax_{k-1} + b$ $(k = 1, \ldots, n)$ par des facteurs convenables).

b) Étudier la suite (x_n); donner sa limite lorsqu'elle en a une.

3.48 On reprend la suite de l'exercice 3.46 en posant toutefois $u_0 = 2 \sin x_0$ $\left(0 \leqslant x_0 \leqslant \dfrac{\pi}{2}\right)$.

a) Démontrer qu'il existe une suite unique (x_n) de nombres réels appartenant à $\left[0, \dfrac{\pi}{2}\right]$ telle que, pour tout n, on ait $u_n = 2 \sin x_n$.

b) Calculer x_{n+1} en fonction de x_n. En déduire la limite de la suite (u_n) (appliquer l'ex. 3.47).

3.49 Soit x un nombre réel tel que $0 < x < \dfrac{\pi}{2}$. On considère la suite (u_n) définie par $u_0 = \cos x$ et, pour tout $n > 0$, par $u_n = u_{n-1} \cos \dfrac{x}{2^n}$.

a) En utilisant la formule $\sin 2a = 2 \sin a \cos a$ calculer u_n à l'aide de n, $\sin 2x$ et $\sin \dfrac{x}{2^n}$.

b) Démontrer que $\dfrac{2^n}{x} \sin \dfrac{x}{2^n}$ a pour limite 1 lorsque n tend vers $+\infty$.

En déduire la limite de (u_n).

3.50 On considère les deux suites (a_n) et (b_n) définies par $a_0 = a > 0$, $b_0 = \dfrac{a}{\cos \alpha}$ $\left(\text{avec } 0 < \alpha < \dfrac{\pi}{2}\right)$ et, pour tout $n > 0$, par

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} \quad , \quad b_n = \sqrt{a_n b_{n-1}}.$$

a) Calculer a_n et b_n en fonction de a et α (utiliser ex. 3.49).

b) Trouver les limites des suites (a_n) et (b_n).

3.51 On considère les deux suites (a_n) et (b_n) définies par $a_0 = a > 0$, $b_0 = b > 0$ et, pour tout $n > 0$, par

$$a_n = \frac{a_{n-1} + b_{n-1}}{2} \quad , \quad b_n = \sqrt{a_{n-1} b_{n-1}}.$$

a) Démontrer que pour tout $n > 0$ on a

$$b_n \leqslant b_{n+1} \leqslant a_{n+1} \leqslant a_n$$

(utiliser ex. 3.1).

b) Démontrer que pour tout $n > 0$ on a

$$a_{n+1} - b_{n+1} \leqslant \frac{a_n - b_n}{2}.$$

En déduire que les deux suites (a_n) et (b_n) ont la même limite l que l'on ne cherchera pas à calculer (l s'appelle la moyenne arithmo-géométrique de GAUSS).

c) *Application numérique.* On donne $a = 2$, $b = 8$. Calculer a_n et b_n pour $n \leqslant 4$.

3.52* On considère une suite (u_n) convergente de limite l et la suite (v_n) définie pour tout $n \geqslant 1$ par

$$v_n = \frac{u_1 + u_2 + \ldots + u_n}{n}.$$

a) Démontrer que $\lim v_n = l$. (Étant donné $\alpha > 0$ il existe p tel que pour tout $k \geqslant p$ on ait $l - \alpha \leqslant u_k \leqslant l + \alpha$; pour $n > p$ on écrira

$$v_n = \frac{u_1 + \ldots + u_{p-1}}{n} + \frac{u_p + \ldots + u_n}{n}\Big).$$

b) Imaginer un contre-exemple montrant que (v_n) peut avoir une limite sans que (u_n) soit convergente.

3.53 On considère la suite (u_n) définie, pour tout $n > 0$, par

$$u_n = \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \ldots + \frac{1}{n(n+1)}.$$

Démontrer que (u_n) est convergente et calculer sa limite.

$$\left(\text{On remarquera que } \frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}\right).$$

3.54 Démontrer que la suite (u_n) définie pour tout $n > 0$ par

$$u_n = \frac{1}{1 \times 3} + \frac{1}{2 \times 4} + \ldots + \frac{1}{n(n+2)}$$

est convergente et calculer sa limite (remarque analogue à celle de ex. 3.53).

3.55* Soit un entier naturel $p \geqslant 1$, on considère la suite définie, pour tout $n > 0$, par

$$u_n = \frac{1}{1^p} + \frac{1}{2^p} + \ldots + \frac{1}{n^p}$$

a) Démontrer que toutes ces suites sont croissantes.

b) On suppose $p = 1$. Démontrer que $u_{2n} - u_n \geqslant \dfrac{1}{2}$. En déduire

$$\lim \left(1 + \frac{1}{2} + \ldots + \frac{1}{n}\right) = +\infty.$$

En déduire l'étude de la suite (v_n) définie, pour tout $n > 0$, par

$$v_n = \frac{1}{1} + \frac{1}{\sqrt{2}} + \ldots + \frac{1}{\sqrt{n}}$$

c) On suppose $p = 2$. Démontrer que (u_n) est majorée. (On remarquera que

$$u_n \leqslant 1 + \frac{1}{1 \times 2} + \frac{1}{2 \times 3} + \ldots + \frac{1}{(n-1)^n}$$

et on utilisera l'ex. 3.53).
En déduire que pour $p = 2$ la suite (u_n) est convergente (on ne cherchera pas à calculer sa limite).
d) Que pensez-vous des suites (u_n) pour $p > 2$?

3.56 On considère la suite (a_n) définie pour tout $n > 0$ par $a_n = \sqrt[n]{n}$.
a) Démontrer que, pour $n \geqslant 2$, on a $a_n > 1$. On pose dans ce cas $n \geqslant 2$, $a_n = 1 + b_n$. Démontrer que

$$(1 + b_n)^n > \frac{n(n-1)}{2} b_n^2.$$

b) Trouver la limite de la suite (b_n) et celle de (a_n).

3.57 On considère la suite (u_n) définie, pour tout entier naturel n, par

$$u_n = \frac{1}{\sqrt{n^2+1}} + \frac{1}{\sqrt{n^2+2}} + \ldots + \frac{1}{\sqrt{n^2+n}}.$$

Démontrer que $\dfrac{n}{\sqrt{n^2+n}} \leqslant u_n \leqslant \dfrac{n}{\sqrt{n^2+1}}$.
En déduire que la suite (u_n) a une limite que l'on calculera.

3.58 Soit la suite (u_n) définie, pour tout n supérieur à la plus grande racine de $x^2 + ax + b$, par $u_n = \sqrt{n^2 + 3n + 7} - \sqrt{n^2 + an + b}$. Montrer que (u_n) a toujours une limite que l'on calculera (a et b paramètres réels).

Pour toute la suite on donne

$$\sqrt{2} = 1{,}414\,214 \ldots \quad \sqrt{3} = 1{,}732\,051 \ldots \quad \sqrt{5} = 2{,}236\,068 \ldots$$
$$\pi = 3{,}141\,592 \ldots \quad e = 2{,}718\,281 \ldots$$

On utilisera dans chaque cas les décimales dont on aura besoin.

On remplace le nombre x par l'une des valeurs approchées a, b, c ou d; indiquer le sens de l'approximation et l'incertitude dans chaque cas (ex. 3.59 à 3.63).

3.59 $x = \sqrt{2}$, $a = \dfrac{7}{5}$, $b = \dfrac{17}{12}$, $c = \dfrac{99}{70}$.

3.60 $x = \sqrt{3}$, $a = \dfrac{7}{4}$, $b = \dfrac{26}{15}$, $c = \dfrac{97}{56}$.

3.61 $x = \sqrt{5}$, $a = \dfrac{9}{4}$, $b = \dfrac{38}{17}$, $c = \dfrac{161}{72}$.

3.62 $x = e$, $a = \dfrac{19}{7}$, $b = \dfrac{87}{32}$, $c = \dfrac{193}{71}$.

3.63 $x = \pi$, $a = \dfrac{22}{7}$, $b = \dfrac{336}{106}$, $c = \dfrac{355}{113}$.

3.64 On prend $e' = 2{,}718$ valeur approchée de e et $\pi' = 3{,}142$ valeur approchée de π.
Déterminer pour e' et π' le sens de l'approximation et l'incertitude.
Avec ces valeurs donner un encadrement de $\dfrac{e}{\pi}$.

3.65 On prend les valeurs approchées 3,142 pour π, 1,414 pour $\sqrt{2}$, 1,732 pour $\sqrt{3}$ donner un encadrement pour $\dfrac{\pi\sqrt{3}}{\sqrt{3}-\sqrt{2}}$.

3.66 *a*) On prend $x' = 3{,}141$ pour π et $y' = 2{,}718$ pour e. Trouver un encadrement de $\pi + e$.

b) On prend $x'' = 3{,}141$ pour π et $y'' = 2{,}71\,828$ pour e. Trouver un encadrement de $\pi + e$.

c) Déduire des calculs précédents que pour avoir sur $x + y$ une incertitude ε il peut être avantageux de prendre x et y avec la même incertitude $\dfrac{\varepsilon}{2}$.

3.67 *a*) x' est une valeur approchée de x avec l'incertitude α. Quelle est l'incertitude lorsque l'on remplace kx par kx'?

b) Trouver une valeur approchée de $3\pi + 10\sqrt{2}$ avec une incertitude inférieure à 10^{-4}. (Appliquer la remarque du 3.65 c).

L'incertitude sur le produit xy de deux nombres positifs est $hy + kx$ (notations du § 3.24 b). Si on veut $kx + hy < l$ ($l > 0$ donné) dans certains cas il peut être avantageux de prendre $kx < \dfrac{l}{2}$ et $hy < \dfrac{l}{2}$; dans d'autres en revanche il sera plus avantageux de prendre l'un des nombres kx ou hy négligeable devant l'autre.

3.68 Trouver une valeur approchée de $\pi\sqrt{2}$ avec une incertitude inférieure à 10^{-4}.

3.69 Trouver une valeur approchée de $\dfrac{e}{2\pi}$ avec une incertitude inférieure à 10^{-4}.

3.70 L'encadrement $4{,}271 < R < 4{,}274$ provient d'une mesure. Donner une valeur approchée de $l = 2\pi R$, $s = \pi R^2$ et $v = \dfrac{4}{3}\pi R^3$ en choisissant chaque fois pour π une valeur approchée telle que l'erreur provenant de π soit le centième de l'erreur provenant de R.

3.71 Les encadrements $3{,}75 < R < 3{,}76$ et $8{,}27 < h < 8{,}29$ proviennent de deux mesures. Donner une valeur approchée de $s = 2\pi R h$ et $v = \pi R^2 h$ en choisissant chaque fois pour π une valeur approchée telle que l'erreur provenant de π soit le centième de la somme des erreurs provenant de R et h.

3.72 On donne $0 < a < x < a + h = a(1 + \alpha)$.

a) Démontrer que $\sqrt{a} < \sqrt{x} < \sqrt{a}\left(1 + \dfrac{\alpha}{2}\right)$.

b) En déduire que l'incertitude sur $\sqrt{x}$ est

$$k = \frac{h}{2\sqrt{x}} \simeq \frac{h}{2\sqrt{a}}.$$

3.73 On donne la formule $T = 2\pi\sqrt{\dfrac{l}{g}}$. Dans les calculs suivants on choisira chaque fois une valeur approchée de π de manière que l'erreur provenant de π soit le centième de la somme des autres erreurs.

a) On donne $0{,}99 < l < 1{,}01$ et $9{,}81 < g < 9{,}82$.
Calculer un encadrement pour T.

b) On donne $0{,}999 < T < 1{,}001$ et $9{,}81 < g < 9{,}82$.
Calculer un encadrement pour l.

c) On donne $0{,}99 < l < 1{,}01$ et l'incertitude sur 1 000 T est 0,5; calculer l'incertitude sur g.

3.74 On pose :

$$(1)\quad y = \frac{1}{99 + 70\sqrt{2}}\ ,\quad (2)\quad z = 99 - 70\sqrt{2}.$$

a) Vérifier que $y = z$.

b) L'incertitude sur $\sqrt{2}$ étant h, calculer l'incertitude sur y calculé par la formule (1), puis l'incertitude sur y calculé par la formule (2).

3.75 Soit les entiers a, b, x tels que $a > 0$, $x > 0$, $a^2 - xb^2 > 0$.
On pose

$$y = \frac{1}{a + b\sqrt{x}} \quad (1) \qquad y = \frac{a - b\sqrt{x}}{a^2 - b^2 x} \quad (2).$$

L'incertitude sur $\sqrt{x}$ étant h, comparer les incertitudes sur y calculé par la formule (1) puis par la formule (2).

Sujets d'étude.

3.76 On se propose de trouver tous les homomorphismes f du corps $(\mathbb{R}, +, \times)$ dans lui-même.

a) Démontrer que, s'il existe a de $\mathbb{R}$ tel que $f(a) \neq 0$, alors $f(1) = 1$, *ce que l'on supposera dans la suite.*

b) Démontrer que, pour tout n de $\mathbb{Z}$, $f(n) = n$ (on commencera par supposer $n \in \mathbb{N}$).

Démontrer que, pour tout n de $\mathbb{N}^*$, on a $f\left(\frac{1}{n}\right) = \frac{1}{n}$.

En déduire que pour tout x de $\mathbb{Q}$ on a $f(x) = x$.

c) Démontrer que, pour tout x de $\mathbb{R}_+$, on a $f(x) \geqslant 0$ (remarquer que $x = (\sqrt{x})^2$). En déduire que f est une application croissante.

d) Démontrer que, pour tout x de $\mathbb{R}$, on a $f(x) = x$. (On définira x comme borne commune à deux suites adjacentes de nombres rationnels).

e) Conclure : Tout homomorphisme du corps $\mathbb{R}$ dans lui-même, distinct de l'application nulle, est l'application identique.

3.77 On dit que le développement *décimal illimité* $x = p_0, \alpha_1, \alpha_2 \ldots \alpha_n \ldots$ est périodique, s'il existe des entiers k et h tels que pour tout $n > k$ on ait $\alpha_{n+h} = \alpha_n$. On a alors

(1) $$x = p_0, \alpha_1 \ldots \alpha_k \alpha_{k+1} \ldots \alpha_{k+h} \alpha_{k+1} \ldots \alpha_{k+h} \ldots$$

$p_0, \alpha_1 \ldots \alpha_k$ est la partie irrégulière et $\alpha_{k+1} \ldots \alpha_{k+h}$ la période.

a) Démontrer que le développement décimal illimité de $\frac{419}{990}$ est périodique.

b) On pose $x = 0{,}3181818\ldots$ (période 18). Démontrer que x est rationnel non décimal. (On pourra poser $x = 0{,}3 + y$ et montrer que $100\,y = 1{,}8 + y$ ou utiliser une suite géométrique de raison 10^{-2}.

c) Démontrer que le développement décimal de tout rationnel non décimal $\frac{p}{q}$ est périodique, la période n'étant ni 0 ni 9. (On remarquera que dans toute division euclidienne par q il y a seulement $q - 1$ restes non nuls possibles).

d) On donne x par le développement décimal (1) où la période n'est ni 0 ni 9. Démontrer que x est rationnel non décimal.

e) Conclure. Le résultat obtenu est-il valable en base a?

4| Nombres complexes.

Le programme prévoit l'introduction des nombres complexes à l'aide de l'ensemble des matrices réelles $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ *muni de l'addition et de la multiplication des matrices.*

Nous avons cru rendre service au lecteur en donnant dans la **Section I** *un résumé des définitions et des principaux résultats concernant les* **espaces vectoriels** *sur* $\mathbb{R}$. *Nous y avons joint une révision et des compléments sur les* **matrices carrées réelles d'ordre 2.**
La **section II** *développe les propriétés du* **corps** $\mathbb{C}$ **des nombres complexes.** *Là aussi la représentation géométrique des complexes est l'occasion de présenter une révision des propriétés du* plan vectoriel euclidien $\mathcal{E}_2$ *et du* plan euclidien E_2. *La section se termine par l'étude du* module *d'un nombre complexe.*
La **section III** *débute par une révision des notions de rotation, d'angle etc... ces notions conduisent à la* **représentation trigonométrique** *d'un nombre complexe et aux calculs utilisant cette forme : produits, quotients, puissances entières, racines* $n^{\text{èmes}}$. *L'utilisation des fonctions trigonométriques nous a incité à présenter un tableau des principales formules de trigonométrie.*

I. Algèbre linéaire (Révisions et compléments)

4. 1 ESPACES VECTORIELS SUR LE CORPS $\mathbb{R}$

a) Définition.

Un espace vectoriel sur le corps $\mathbb{R}$ est un ensemble E muni d'une loi interne notée $\perp$, d'une loi externe associant à tout couple (α, a) de $\mathbb{R} \times E$ un élément de E noté $\alpha \star a$, vérifiant les propriétés suivantes :

1. (E, $\perp$) est un groupe abélien.
2. Quels que soient a de E, α et β de $\mathbb{R}$ on a
$$1 \star a = a,$$
$$\alpha \star (\beta \star a) = (\alpha . \beta) \star a.$$
3. Quels que soient a, b de E et α, β de $\mathbb{R}$, on a
$$\alpha \star (a \perp b) = (\alpha \star a) \perp (\alpha \star b),$$
$$(\alpha + \beta) \star a = (\alpha \star a) \perp (\beta \star a).$$

Pour des raisons de simplification d'écriture, nous noterons avec le même signe $+$ l'*addition* dans $\mathbb{R}$ et l'opération interne de E, appelée addition dans E; de même nous noterons par le même signe . la multiplication dans $\mathbb{R}$ et la **multiplication externe.**

En fait dans la pratique on note $\alpha\beta$ le produit de deux éléments de $\mathbb{R}$ et αa le composé par la multiplication externe de $\alpha \in \mathbb{R}$ et $a \in E$.
D'autre part, notons 0_E l'élément neutre du groupe $(E, +)$ et $(-a)$ l'*opposé* de a dans E.
Avec ces notations, les **axiomes d'un espace vectoriel sur** $\mathbb{R}$, traduisant les propriétés (1), (2), (3) ci-dessus, s'énoncent comme suit :

V_1. *Quels que soient* a, b, c *de* E *on a*

$$(a + b) + c = a + (b + c).$$

V_2. *Quels que soient* a, b *de* E *on a*

$$a + b = b + a.$$

V_3. *Il existe* $0_E \in E$, *tel que, quel que soit* a *de* E *on ait* :

$$a + 0_E = 0_E + a = a.$$

V_4. *Pour tout élément* a *de* E, *il existe un élément* $(-a)$ *de* E *tel que l'on ait* :

$$a + (-a) = (-a) + a = 0_E.$$

V_5. *Pour tout élément* a *de* E *on a*

$$1 . a = a.$$

V_6. *Quels que soient* a *de* E *et* α, β *de* $\mathbb{R}$ *on a*

$$\alpha (\beta a) = (\alpha\beta) a.$$

V_7. *Quels que soient* a *de* E *et* α, β *de* $\mathbb{R}$ *on a*

$$(\alpha + \beta) a = (\alpha a) + (\beta a).$$

V_8. *Quels que soient* a, b *de* E *et* α *de* $\mathbb{R}$ *on a*

$$\alpha (a + b) = (\alpha a) + (\alpha b).$$

V_1, V_2, V_3, V_4 expriment que $(E, +)$ est un groupe commutatif. (On dit aussi que $(E, +)$ est un groupe abélien).
V_5 et V_6 correspondent à l'axiome (2) de la définition.
V_7 et V_8 correspondent à l'axiome (3) de la définition.

Ces huit propriétés sont les axiomes de la structure d'espace vectoriel sur $\mathbb{R}$.

Bien que nous écrivions αa sans point entre α et a, nous noterons $(E, +, \bullet)$ tout espace vectoriel sur $\mathbb{R}$.
Si, dans ces huit axiomes nous substituons à $\mathbb{R}$ un corps commutatif quelconque **K, en** remplaçant 1 par l'élément unité e de K, nous obtenons les huit axiomes de la structure d'**espace vectoriel sur le corps commutatif** K.
Les éléments de E sont appelés **vecteurs,** ceux de K **scalaires.**

EXERCICE

1. Pour chacun des ensembles E suivants indiquer l'addition et la multiplication externe telle que $(E, +, \bullet)$ soit un espace vectoriel sur K.
   — Ensemble des fonctions binômes à coefficients réels ($K = \mathbb{R}$)
   — Ensemble des fonctions trinômes à coefficients réels ($K = \mathbb{R}$)
   — $\mathcal{F}(X, \mathbb{R})$ où X est un ensemble quelconque ($K = \mathbb{R}$). On pourra étudier les cas suivants : X est un intervalle de $\mathbb{R}$ et en particulier $X = \mathbb{R}$.
   — $\mathbb{R}$ ($K = \mathbb{R}$)
   — $\mathbb{R}$ ($K = \mathbb{Q}$)
   — $\mathbb{R} \times \mathbb{R}$ ($K = \mathbb{R}$)
   — $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$ ($K = \mathbb{R}$)
   — $\mathbb{Z}5/\mathbb{Z} \times \mathbb{Z}/5\,\mathbb{Z}$ ($K = 5\mathbb{Z}/\mathbb{Z}$)

b) Règles de calcul dans un espace vectoriel.

Nous avons d'abord les règles de calcul dans un groupe abélien. Quels que soient a, b, c, x de E, on a

$$(a = b) \iff (a + c = b + c)$$
$$(x + b = a) \iff (x = a + (-b) = a - b)$$
$$-(a + b) = (-a) + (-b)$$

Quels que soient $\alpha \in \mathbb{R}$ et $x \in E$, on a

$$(\alpha x = 0_E) \iff (\alpha = 0_K \text{ ou } x = 0_E).$$

Ceci montre qu'il n'y a aucun inconvénient à noter 0 l'élément neutre de $\mathbb{R}$ et celui de E.

Quels que soient α, β de $\mathbb{R}$ et x, y de E, on a

$$(-\alpha)\, x = \alpha\,(-x) = -(\alpha x).$$

Ces trois symboles représentent le même élément de E que l'on notera simplement $-\alpha x$; en particulier $(-1)\, x$ s'écrit $-x$.

On a aussi

$$(\alpha - \beta)\, x = \alpha x - \beta x,$$
$$\alpha\,(x - y) = \alpha x - \alpha y.$$

Soit $n \geqslant 1$ scalaires $\alpha_1, \alpha_2, \ldots, \alpha_n$ et n vecteurs $a_1, a_2, \ldots, a_n$, le vecteur

$$x = \alpha_1 a_1 + \ldots + \alpha_n a_n = \sum_{k=1}^{k=n} \alpha_k a_k$$

est appelé **combinaison linéaire** des n vecteurs $a_1, \ldots, a_n$; $\alpha_1, \ldots, \alpha_n$ sont les *coefficients* respectifs de $a_1, \ldots, a_n$ dans cette combinaison linéaire.

c) Sous-espaces vectoriels.

Définitions.

1. Étant donné E, espace vectoriel sur $\mathbb{R}$, on dit qu'une partie S de E est **stable** pour la multiplication externe si et seulement si, pour tout $\alpha \in \mathbb{R}$ et tout $x \in S$, on a $\alpha x \in S$.
2. On dit que F partie de E est un **sous-espace vectoriel** de E si et seulement si
   i. F est stable pour l'addition et la multiplication externe
   ii. (F, +, •) est un espace vectoriel sur $\mathbb{R}$.

Nous avons établi le théorème suivant :

Théorème.

Soit E un espace vectoriel sur $\mathbb{R}$; toute partie F de E est un sous-espace vectoriel de E si et seulement si les propriétés suivantes sont simultanément vérifiées :
i. F est non vide,
ii. F est une partie stable de E pour l'addition,
iii. F est une partie stable de E pour la multiplication externe.

Si F est une partie **non vide** de E, F est donc un sous-espace vectoriel de E si et seulement si, quels que soient α, β de $\mathbb{R}$ et x, y de F, on a

$$\alpha x + \beta y \in F.$$

Les sous-ensembles $\{0_E\}$ et E sont des sous-espaces vectoriels de E. Tout autre sous-espace vectoriel de E est appelé *sous-espace vectoriel propre* de E.

Si $A = \{a_1, a_2, \ldots a_n\}$ est un sous-ensemble d'éléments de E, l'ensemble des combinaisons linéaires des éléments de A est un sous-espace vectoriel de E, appelé **sous-espace vectoriel engendré par** A.

EXERCICE

2. En utilisant les exemples de l'exercice 1 ci-dessus indiquer des couples (E, F) où F est un sous-espace vectoriel de E.

4. 2 FAMILLES GÉNÉRATRICES. FAMILLES LIBRES. BASES

a) Familles génératrices - Bases.

Définition.

La famille $A = (a_1, \ldots, a_n)$ de E espace vectoriel sur $\mathbb{R}$ est une famille **génératrice** de l'espace vectoriel E si et seulement si le sous-espace vectoriel engendré par A est égal à E.

Autrement dit, tout élément de E peut s'exprimer comme combinaison linéaire des éléments de A.

Définition.

On appelle **base** d'un espace vectoriel E sur $\mathbb{R}$ toute famille génératrice $A = (a_1, \ldots, a_n)$ de E telle que tout élément de E est combinaison linéaire de $a_1, \ldots, a_n$ d'une manière unique.

EXERCICES

1. Soit $A = ((1, -1, 0), (1, 2, 1), (2, 1, 1))$ une famille de $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. A est-elle une famille génératrice de $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$? Est-elle une base?

2. Mêmes questions avec $E = \mathbb{R} \times \mathbb{R}$ et $A = ((1, 2), (3, -1), (4, 1))$.

b) Dépendance et indépendance linéaire.

Définition 1.

Les éléments $a_1, \ldots, a_p$ de E sont dits **linéairement indépendants** si et seulement si, quels que soient les nombres réels $\alpha_1, \alpha_2, \ldots, \alpha_p$, on a :

$$(\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_p a_p = 0_E) \Longrightarrow (\alpha_1 = \alpha_2 = \ldots = \alpha_p = 0);$$

La famille $(a_1, \ldots, a_p)$ de E s'appelle alors **famille libre** de E.

Définition 2.

Les éléments $a_1, \ldots, a_p$ de E sont dits **linéairement dépendants** si et seulement s'il existe des nombres réels $\alpha_1, \alpha_2, \ldots, \alpha_p$ non tous nuls tels que :

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_p a_p = 0_E.$$

La famille $(a_1, \ldots, a_p)$ de E s'appelle alors **famille liée** de E.

Par exemple, (0_E) est une famille liée de E; (a) où $a \neq 0_E$ est une famille libre de E.
Nous avons démontré :

— *Toute famille de* E *contenant une famille liée est elle-même une famille liée.*

— *Tout sous-ensemble d'une famille libre détermine une famille libre.*

Donc tous les éléments d'une famille libre sont distincts de 0_E.

— *Une famille de* E *est liée si et seulement si elle contient un élément combinaison linéaire des autres.*

Nous avons établi le théorème important suivant :

Théorème.

Une famille $(e_1, \ldots, e_n)$ d'un espace vectoriel E sur $\mathbb{R}$ est une base de E si et seulement si c'est une famille génératrice de E et libre.

c) Dimension d'un espace vectoriel sur $\mathbb{R}$.

Toutes les bases d'un espace vectoriel E *ont le même nombre d'éléments.* Ce résultat a été démontré lorsque E admet une base ayant 1, 2 ou 3 éléments.
Ce nombre d'éléments commun à toutes les bases de E s'appelle la *dimension de* E, on le note dim E.

REMARQUE

1. $\{0_E\}$ est un espace vectoriel ne contenant que le vecteur nul. Il n'a donc pas de base. On convient de dire que $\{0_E\}$ est de dimension zéro.

Dans le cas où E est de dimension 1, on dit que E est une *droite vectorielle*. Si sa dimension est 2, on dit que E est un *plan vectoriel.*

Si $(e_1, \ldots, e_n)$ est une base de E tout vecteur x de E s'écrit d'une manière unique

$$x = \alpha_1 e_1 + \ldots + \alpha_n e_n$$

les coefficients $\alpha_1 \ldots \alpha_n$ sont appelés **coordonnées** de x relativement à la base $(e_1, \ldots, e_n)$, α_i étant la coordonnée relative au vecteur e_i de la base.

EXERCICES

3. Soit E un espace vectoriel de dimension $n \geqslant 1$. Démontrer que toute famille $B = (e_1, \ldots, e_p)$ possédant *deux* des propriétés suivantes est une base.
   1. $p = n$.
   2. B est une famille libre de E.
   3. B est une famille génératrice de E.

4. Démontrer que $\mathbb{R}^n$ muni de l'addition

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$$

et de la multiplication externe, dont le domaine d'opérateurs est $\mathbb{R}$,

$$\lambda(\alpha_1, \ldots, \alpha_n) = (\lambda\alpha_1, \ldots, \lambda\alpha_n),$$

est un espace vectoriel sur $\mathbb{R}$.
Pour tout i tel que $1 \leqslant i \leqslant n$, on pose

$$e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0),$$

où 1 est à la i^{eme} place; démontrer que $(e_1, \ldots, e_n)$ est une base de $\mathbb{R}^n$, espace vectoriel sur $\mathbb{R}$, elle est appelée **base canonique** de $\mathbb{R}^n$.
(On pourra commencer par étudier le cas $n = 3$).

Soit F un *sous-espace vectoriel* de E espace vectoriel de dimension $n \geqslant 1$ sur $\mathbb{R}$. Nous avons montré pour $n = 1, 2, 3$ le résultat suivant

$$\dim F \leqslant \dim E.$$

En particulier si $F = \{0_E\}$ on a $\dim F = 0$ et si $F = E$ on a $\dim F = n$.
Réciproquement si F est un sous-espace vectoriel de E tel que $\dim F = \dim E$, on a $F = E$.

d) Intersection de deux sous-espaces vectoriels de E.

L'intersection de deux sous-espaces vectoriels de E *est un sous-espace vectoriel de* E.

Plus précisément, nous avons les résultats suivants, concernant deux sous-espaces vectoriels propres F_i et G_j de E :

1° **dim E = 2**

Base de F_1	Base de G_1	Relation entre les vecteurs des bases	$F_1 \cap G_1$
(a_1)	(b_1)	(a_1, b_1) liée	$F_1 = G_1$
(a_1)	(b_1)	(a_1, b_1) libre	$\{0_E\}$

2° **dim E = 3**

Base de F_i $i = 1$ ou 2	Base de G_j $j = 1$ ou 2	Relation entre les vecteurs des bases	$F_i \cap G_j$
(a_1)	(b_1)	(a_1, b_1) liée	$F_1 = G_1$
(a_1)	(b_1)	(a_1, b_1) libre	$\{0_E\}$
(a_1)	(b_1, b_2)	(a_1, b_1, b_2) liée	F_1
(a_1)	(b_1, b_2)	(a_1, b_1, b_2) libre	$\{0_E\}$
(a_1, a_2)	(b_1, b_2)	(a_1, b_1, b_2) liée et (a_2, b_1, b_2) liée	$F_2 = G_2$
(a_1, a_2)	(b_1, b_2)	(a_1, b_1, b_2) libre ou (a_2, b_1, b_2) libre	$\Delta(c)$

$\Delta(c)$ désignant une droite vectorielle.

EXERCICE

5. Soit $\mathcal{F}$ une famille non vide finie ou infinie de sous-espaces vectoriels F de E. Soit I l'intersection de *tous* les sous espaces F de la famille $\mathcal{F}$. Démontrer que I est un sous-espace vectoriel de E.

4. 3 APPLICATIONS LINÉAIRES

a) Définition. Exemples.

Définition.

Étant donnés deux espaces vectoriels E et F sur $\mathbb{R}$, l'application f de E dans F est une **application linéaire** si et seulement si les deux propriétés suivantes sont réalisées : quels que soient x_1 et x_2 de E et quel que soit α de $\mathbb{R}$, on a

(1) $$f(x_1 + x_2) = f(x_1) + f(x_2),$$

(2) $$f(\alpha\, x_1) = \alpha\, f(x_1).$$

On dit aussi que f est un homomorphisme de l'espace vectoriel E dans l'espace vectoriel F. La relation (1) montre que f est, en particulier, un homomorphisme du groupe (E, +) dans le groupe (F, +).

EXEMPLES

1. Soit E un espace vectoriel de dimension 2, de base $(\vec{i}, \vec{j})$. Dans cette base, un vecteur $\vec{v}$ peut s'écrire, de façon unique, sous la forme $\vec{v} = x\vec{i} + y\vec{j}$; x et y désignent les *coordonnées* de $\vec{v}$ dans la base $(\vec{i}, \vec{j})$.
   L'application : $E \longrightarrow \mathbb{R} \times \mathbb{R}$
   définie par : $\vec{v} \longmapsto (x, y)$
   est une application linéaire de E dans $\mathbb{R} \times \mathbb{R}$. On le vérifiera.

2. Avec les mêmes notations qu'à l'exemple 1 ci-dessus, l'application p_1 de E dans $\mathbb{R}$ définie pour tout $\vec{v}$ de E par $p_1(\vec{v}) = x$, est une application linéaire, ce que l'on vérifiera. Elle est appelée *première projection* de E sur $\mathbb{R}$.
   De même, l'application p_2 définie pour tout $\vec{v}$ de E par : $p_2(\vec{v}) = y$ est linéaire. On l'appelle *deuxième projection* de E sur $\mathbb{R}$.

b) Premières propriétés des applications linéaires.

Nous ne rappellerons ici que les propriétés nécessaires pour définir le corps des nombres complexes.
Soit trois espaces vectoriels E, F, G sur $\mathbb{R}$ et les deux applications linéaires

$$E \xrightarrow{f} F \xrightarrow{g} G$$

alors $g \circ f$ est une application linéaire de E dans G, autrement dit la *composée de deux applications linéaires est linéaire.*

D'autre part, pour toute application linéaire f de E dans F, on a

$$f(0_E) = 0_F$$

et, quel que soit x de E, on a

$$f(-x) = -f(x).$$

EXERCICE

1. Soit f une application linéaire de E dans F, E et F espaces vectoriels sur $\mathbb{R}$.

   a) Démontrer que $I = f(E)$ est un sous espace vectoriel de F appelé **image de** f.

   b) Démontrer que N ensemble des vecteurs x de E vérifiant $f(x) = 0_F$ est un sous-espace vectoriel de E appelé **noyau de** f.
   Démontrer que f est injective si et seulement si $N = \{0_E\}$.

c) Isomorphismes d'espaces vectoriels.

Nous poserons la définition suivante :

Définition.

Étant donnés les espaces vectoriels E et F sur $\mathbb{R}$ on dit que l'application linéaire $f : E \longrightarrow F$ est un **isomorphisme** si et seulement si

i. L'application f est bijective.

ii. L'application f^{-1} est une application linéaire de F sur E.

Nous avons démontré les résultats suivants :

Théorème.

Pour que l'application linéaire

$$f : E \longrightarrow F$$

soit un isomorphisme d'espaces vectoriels il faut et il suffit que f soit bijective.

Corollaire.

Le composé de deux isomorphismes d'espaces vectoriels est un isomorphisme d'espaces vectoriels.

d) Complément. Anneau $(\mathcal{L}(E), +, \circ)$.

Le contenu de ce sous-paragraphe est nouveau par rapport au cours de Première.

Désignons par $\mathcal{L}(E)$ l'ensemble des applications linéaires de E espace vectoriel sur $\mathbb{R}$ dans lui-même.
Si f et g appartiennent à $\mathcal{L}(E)$ nous savons qu'il en est de même de $f \circ g$; la **composition** des applications, est donc une loi interne définie sur $\mathcal{L}(E)$. Elle est associative; elle admet l'élément neutre $e = \mathrm{id}_E$ et nous avons vu en Première que si $\dim E \geqslant 2$ cette loi n'est pas commutative.

Nous définirons une **addition** dans $\mathcal{L}(E)$ en posant, quels que soient f et g de $\mathcal{L}(E)$

$$(\forall\, x \in E) \quad (f+g)(x) = f(x) + g(x).$$

EXERCICE

2. Démontrer que, quels que soient x et y de E et α de $\mathbb{R}$, on a

$$(f+g)(x+y) = (f+g)(x) + (f+g)(y)$$
$$(f+g)(\alpha x) = \alpha (f+g)(x)$$

Le résultat de cet exercice montre que l'addition est une loi interne définie sur $\mathcal{L}(E)$.

EXERCICE

3. Démontrer que $(\mathcal{L}(E), +)$ est un groupe abélien.
   L'élément neutre ω est l'**application nulle,** qui est évidemment linéaire; elle est définie par

$$(\forall\, x \in E) \quad \omega(x) = 0_E.$$

L'opposée de f notée $-f$ est définie par

$$(\forall\, x \in E) \quad (-f)(x) = -f(x)$$

c'est une application linéaire.

Considérons maintenant $(\mathcal{L}(E), +, \circ)$; d'après les résultats obtenus déjà si nous montrons que la composition est distributive par rapport à l'addition nous aurons montré que $(\mathcal{L}(E), +. \circ)$ est un anneau.

La composition n'étant pas commutative, il faut montrer que la composition est distributive à gauche et à droite par rapport à l'addition.

Soit f, g_1, g_2 des éléments quelconques de $\mathcal{L}(E)$; on a pour tout x,

$$\begin{aligned}
[f \circ (g_1 + g_2))(x) &= f[(g_1 + g_2)(x)] && \text{(définition de } f \circ (g_1 + g_2)\text{).}\\
&= f[g_1(x) + g_2(x)] && \text{(définition de } g_1 + g_2\text{)}\\
&= f[g_1(x)] + f[g_2(x)] && \text{(linéarité de } f\text{)}\\
&= (f \circ g_1)(x) + (f \circ g_2)(x) && \text{(définition de } f \circ g_1 \text{ et } f \circ g_2\text{)}\\
&= (f \circ g_1 + f \circ g_2)(x) && \text{(définition de } f \circ g_1 + f \circ g_2\text{).}
\end{aligned}$$

Il en résulte que

$$f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2.$$

Vous démontrerez de même que, quelles que soient les applications linéaires f_1, f_2, g de E dans E, on a

$$(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g.$$

Il en résulte de toutes ces propriétés

$(\mathcal{L}(E), +, \circ)$ est un anneau unitaire.

Cet anneau est non commutatif si $\dim E \geqslant 2$.

EXERCICE

4. On désigne par $\mathcal{H}(E)$ l'ensemble des homothéties de l'espace vectoriel E. On rappelle que l'homothétie f_λ est définie pour tout x de E par $f_\lambda(x) = \lambda x$.
Démontrer que $(\mathcal{H}(E), +, \circ)$ est un sous-anneau de $(\mathcal{L}(E), +, \circ)$.
Démontrer que l'application φ

$$\begin{aligned}
\varphi : \mathbb{R} &\longrightarrow \mathcal{H}(E)\\
\lambda &\longmapsto f_\lambda
\end{aligned}$$

est un isomorphisme de $(\mathbb{R}, +, \times)$ sur $(\mathcal{H}(E), +, \circ)$. En déduire que $(\mathcal{H}(E), +, \circ)$ est un corps commutatif.

Cet exercice nous donne un exemple de sous-anneau, ce sous-anneau ayant une structure de corps commutatif.

4. 4 DÉTERMINATION D'UNE APPLICATION LINÉAIRE. MATRICES

Nous nous limiterons dans ce paragraphe aux applications linéaires de $\mathcal{V}_2$ dans $\mathcal{V}_2$, $\mathcal{V}_2$ *étant un espace vectoriel de dimension 2 sur* $\mathbb{R}$.

a) Détermination d'une application linéaire.

Soit $(\vec{i}, \vec{j})$ une base de $\mathcal{V}_2$. Nous avons vu en Première le résultat suivant :

Quels que soient les vecteurs $\vec{i}_1$ et $\vec{j}_1$ de $\mathcal{V}_2$ il existe une application linéaire unique f de $\mathcal{V}_2$ dqns $\mathcal{V}_2$ telle que

$$f(\vec{i}) = \vec{i}_1, \quad f(\vec{j}) = \vec{j}_1.$$

Autrement dit f est déterminée par $f(\vec{i})$ et $f(\vec{j})$: si $\vec{v} = x\vec{i} + y\vec{j}$ est un vecteur quelconque de $\mathcal{V}_2$ on a

$$f(\vec{v}) = f(x\vec{i} + y\vec{j}) = x f(\vec{i}) + y f(\vec{j}).$$

b) Ensemble $\mathcal{M}_2$ des matrices carrées d'ordre 2.

Les images $f(\vec{i})$ et $f(\vec{j})$ des vecteurs d'une base $(\vec{i}, \vec{j})$ peuvent alors s'exprimer dans cette base. Il existe des nombres réels a, b, c, d tels que :

$$f(\vec{i}) = a\vec{i} + b\vec{j},$$
$$f(\vec{j}) = c\vec{i} + d\vec{j}.$$

Le tableau des coordonnées de $f(\vec{i})$ et $f(\vec{j})$ dans la base $(\vec{i}, \vec{j})$ a été appelé **matrice de l'application f dans la base $(\vec{i}, \vec{j})$**.

$$\mathrm{M}(f, \vec{i}, \vec{j}) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}.$$

L'ensemble des matrices de ce type a été désigné par $\mathcal{M}_2$, ensemble des matrices réelles, à 2 colonnes et 2 lignes.
On dit aussi que $\mathcal{M}_2$ est l'ensemble des **matrices carrées réelles d'ordre** 2.
Une base $(\vec{i}, \vec{j})$ étant choisie dans $\mathcal{V}_2$ nous avons vu que l'application

$$\varphi : \mathfrak{L}(\mathcal{V}_2) \longrightarrow \mathcal{M}_2$$
$$f \longmapsto \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

où $f(\vec{i}) = a\vec{i} + b\vec{j}$ (a, b constituant la 1re colonne) et $f(\vec{j}) = c\vec{i} + d\vec{j}$ (c, d constituant la 2e colonne) est une bijection.

c) Multiplication des matrices carrées d'ordre 2.

Nous avons défini en Première une multiplication dans $\mathcal{M}_2$ de telle manière que la bijection φ définie ci-dessus soit un isomorphisme de $(\mathfrak{L}(\mathcal{V}_2), \circ)$ sur $(\mathcal{M}_2, \times)$. C'est-à-dire si on pose

$$\mathrm{A} = \mathrm{M}(f, \vec{i}, \vec{j}) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$
$$\mathrm{A}' = \mathrm{M}(f', \vec{i}, \vec{j}) = \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$$

on a par définition

$$\mathrm{AA}' = \mathrm{M}(f \circ f', \vec{i}, \vec{j}).$$

Nous avons trouvé

$$\mathrm{AA}' = \begin{pmatrix} aa' + cb' & ac' + cd' \\ ba' + db' & bc' + dd' \end{pmatrix}.$$

D'après l'isomorphisme φ la multiplication des matrices est associative, non commutative et possède l'élément neutre

$$\mathrm{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \mathrm{M}(\mathrm{Id}_{\mathcal{V}_2}, \vec{i}, \vec{j}).$$

Matrices carrées d'ordre 2 inversibles.

Il a été démontré en Première que l'ensemble des applications linéaires bijectives de $\mathcal{V}_2$ dans $\mathcal{V}_2$ est un groupe pour la composition des applications.
Il lui est associé, par bijection φ précédemment indiquée, un sous-ensemble de matrices de $\mathcal{M}_2$, dites **matrices inversibles**, qui constitue un groupe pour la multiplication des matrices.

Nous avons, d'autre part, démontré le théorème important suivant :

Théorème.

Pour toute application linéaire f de $\mathcal{V}_2$ dans $\mathcal{V}_2$, les cinq propriétés suivantes sont équivalentes :

1. L'application linéaire f est bijective.
2. La matrice associée à f dans une base quelconque est inversible.
3. $\det(A) \neq 0$.
4. Le noyau de f est $\{\vec{0}\}$.
5. L'image par f d'une base est une base.

Rappelons que

$$\det \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{vmatrix} a & c \\ b & d \end{vmatrix} = ad - bc.$$

d) Complément. Anneau $(\mathcal{M}_2, +, \times)$.

Le contenu de ce paragraphe est nouveau par rapport au cours de Première.
Procédant comme pour la multiplication nous définirons dans $\mathcal{M}_2$ une addition de manière que la bijection φ définie ci-dessus soit aussi un isomorphisme de $(\mathfrak{L}(\mathcal{V}_2), +)$ sur $(\mathcal{M}_2, +)$.
C'est-à-dire si on pose

$$A = M(f, \vec{i}, \vec{j}) = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$
$$A' = M(f', \vec{i}, \vec{j}) = \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix}$$

on a par définition

$$A + A' = M(f + f', \vec{i}, \vec{j}).$$

On aura donc

$$(f+f')(\vec{i}) = f(\vec{i}) + f'(\vec{i}) = (a\vec{i} + b\vec{j}) + (a'\vec{i} + b'\vec{j})$$
$$= (a + a')\vec{i} + (b + b')\vec{j}$$
$$(f+f')(\vec{j}) = f(\vec{j}) + f'(\vec{j}) = (c\vec{i} + d\vec{j}) + (c'\vec{i} + d'\vec{j})$$
$$= (c + c')\vec{i} + (d + d')\vec{j}$$

d'où

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} + \begin{pmatrix} a' & c' \\ b' & d' \end{pmatrix} = \begin{pmatrix} a + a' & c + c' \\ b + b' & d + d' \end{pmatrix}$$

Nous avons vu que $(\mathfrak{L}(\mathfrak{V}_2), +)$ est un groupe abélien (cf. § 4.3 d en faisant $E = \mathfrak{V}_2$); l'isomorphisme φ de $(\mathfrak{L}(\mathfrak{V}_2), +)$ sur $(\mathcal{M}_2, +)$ nous montre que $(\mathcal{M}_2, +)$ est un groupe abélien. L'élément neutre est

$$O = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

appelée **matrice nulle** (sous-entendu matrice carrée d'ordre 2).
L'opposée de A notée $-A$ est telle que

$$-\begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} -a & -c \\ -b & -d \end{pmatrix}.$$

Nous pouvons considérer maintenant $(\mathcal{M}_2, +, \times)$; la bijection φ de $\mathfrak{L}(\mathfrak{V}_2)$ sur $\mathcal{M}_2$ étant à la fois un isomorphisme de $(\mathfrak{L}(\mathfrak{V}_2), +)$ sur $(\mathcal{M}_2, +)$ et de $(\mathfrak{L}(\mathfrak{V}_2), \circ)$ sur $(\mathcal{M}_2, \times)$, les relations (cf. § 4.3 d)

$$f \circ (g_1 + g_2) = f \circ g_1 + f \circ g_2$$
$$(f_1 + f_2) \circ g = f_1 \circ g + f_2 \circ g$$

entraînent, avec des notations évidentes,

$$A(B_1 + B_2) = AB_1 + AB_2$$
$$(A_1 + A_2)B = A_1B + A_2B.$$

Il en résulte que

$(\mathcal{M}_2, +, \times)$ est un anneau unitaire.

Cet anneau est non commutatif.

II. Corps des nombres complexes $\mathbb{C}$

4. 5 DÉFINITION. OPÉRATIONS DANS $\mathbb{C}$

Considérons l'ensemble $\mathbb{C}$ des matrices à 2 colonnes et 2 lignes qui s'écrivent $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ où a et b sont des nombres réels quelconques.
Dans ce sous-ensemble de $\mathcal{M}_2$, nous allons étudier les deux opérations précédemment définies : addition et multiplication.
Nous donnerons d'abord des démonstrations utilisant les résultats des § *4.3* d et § *4.4* d; *nous donnerons ensuite des démonstrations directes en utilisant uniquement la formule donnant la somme de deux matrices, ceci pour les lecteurs qui n'auraient pas étudié les* § *4.3* d *et 4.4* d.

a) Addition dans $\mathbb{C}$.

D'après la définition de l'addition dans $\mathcal{M}_2$ donnée précédemment on a

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} + \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a + a' & -(b + b') \\ b + b' & a + a' \end{pmatrix} \quad (1)$$

La somme de deux matrices de $\mathbb{C}$ est donc une matrice de $\mathbb{C}$ (il suffit de poser $a'' = a + a'$ et $b'' = b + b'$).
L'addition des matrices est donc une opération interne dans $\mathbb{C}$.
L'ensemble $\mathbb{C}$ est une partie non vide de $\mathcal{M}_2$; quels que soient les éléments A et A' de $\mathbb{C}$ on a $A - A' \in \mathbb{C}$ (le vérifier); donc $(\mathbb{C}, +)$ est un sous-groupe du groupe abélien $(\mathcal{M}_2, +)$.

Conclusion : $(\mathbb{C}, +)$ est un *groupe abélien.*

Voici les démonstrations directes fondées uniquement sur la formule (1) *pour les lecteurs n'ayant pas étudié les* § 4.3 d et 4.4 d.
Il est évident, d'après la formule (1) que l'addition est une opération commutative (puisque l'addition dans $\mathbb{R}$ est commutative), associative (puisque l'addition dans $\mathbb{R}$ est associative), on fera aisément le calcul.

Il existe un élément neutre $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ appelé « matrice nulle » et qu'on notera O.

La matrice symétrique de $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est $\begin{pmatrix} -a & -b \\ -b & a \end{pmatrix}$. On l'appelle son *opposée*; on vérifie qu'elle fait partie de $\mathbb{C}$. Toute matrice de $\mathbb{C}$ admet donc une opposée qui appartient à $\mathbb{C}$. Il résulte de ces propriétés que $(\mathbb{C}, +)$ est un groupe abélien.

b) Multiplication dans $\mathbb{C}$.

D'après la définition du produit de deux matrices de $\mathcal{M}_2$, nous obtenons :

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} aa' - bb' & -(ba' + ab') \\ ba' + ab' & aa' - bb' \end{pmatrix}. \qquad (2)$$

La multiplication des matrices est donc une *opération interne* dans $\mathbb{C}$ (il suffit de poser $a'' = aa' - bb'$, $b'' = ab' + a'b$). Nous remarquons, d'autre part, que quelles que soient les matrices de $\mathbb{C}$ considérées on a

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} \times \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

La multiplication des matrices de $\mathbb{C}$ est donc *commutative*. La multiplication étant *associative* dans $\mathcal{M}_2$, elle l'est dans $\mathbb{C}$. L'élément neutre $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ appartient à $\mathbb{C}$ $(a = 1, \quad b = 0)$.

Cherchons les *matrices inversibles* de $\mathbb{C}$. Nous savons que $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ est inversible si et seulement si (cf § 4.4 c)

$$\det A = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0.$$

Or, dans $\mathbb{R}$, tout carré étant positif, $a^2 + b^2 = 0$ si et seulement si $(a, b) = (0, 0)$, c'est-à-dire si et seulement si $A = O$.
Donc *toute matrice non nulle* A *de* $\mathbb{C}$ *admet une matrice inverse* A^{-1}. Tout ce que nous savons, pour l'instant, c'est que $A^{-1} \in \mathcal{M}_2$. Nous allons voir que $A^{-1} \in \mathbb{C}$. Montrons que si $a^2 + b^2 \neq 0$ il existe des réels a', b' tels que

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

On devra avoir

$$\begin{cases} aa' - bb' = 1, \\ ba' + ab' = 0 \end{cases}$$

d'où l'on déduit

$$\begin{cases} a' = \dfrac{a}{a^2 + b^2}, \\ b' = \dfrac{-b}{a^2 + b^2}. \end{cases}$$

Par suite, la matrice inverse de $A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ où $a^2 + b^2 \neq 0$ appartient à $\mathbb{C}$ et elle est égale à

$$A^{-1} = \begin{pmatrix} \dfrac{a}{a^2 + b^2} & \dfrac{b}{a^2 + b^2} \\ \dfrac{-b}{a^2 + b^2} & \dfrac{a}{a^2 + b^2} \end{pmatrix}.$$

Posons $\mathbb{C}^* = \mathbb{C} - \{0\}$ nous pouvons conclure : $(\mathbb{C}^*, \times)$ est un *groupe abélien.*

EXERCICE

Déterminer A^{-1} pour

$$A = \begin{pmatrix} 2 & -3 \\ 3 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \text{ avec } \lambda \neq 0, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

c) Corps commutatif $(\mathbb{C}, +, \times)$.

$\mathbb{C}$ est une partie stable de $\mathcal{M}_2$ pour l'addition et la multiplication des matrices; or nous avons vu que dans $(\mathcal{M}_2, +, \times)$ la multiplication est *distributive* par rapport à l'addition, il en est de même dans $\mathbb{C}$.

Dans $(\mathbb{C}, +, \times)$ *la multiplication est distributive par rapport à l'addition.*

Voici un calcul direct pour les lecteurs qui n'auraient pas étudié les § 4.3 d et 4.4 d. Pour trois matrices quelconques de $\mathbb{C}$, comparons :

$$A = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \left[\begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a'' & -b'' \\ b'' & a'' \end{pmatrix} \right]$$

et

$$B = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' & -b' \\ b' & a' \end{pmatrix} + \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a'' & -b'' \\ b'' & a'' \end{pmatrix}.$$

On a d'une part

$$\begin{aligned} A &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \times \begin{pmatrix} a' + a'' & -(b' + b'') \\ b' + b'' & a' + a'' \end{pmatrix}, \\ &= \begin{pmatrix} a(a' + a'') - b(b' + b'') & -a(b' + b'') - b(a' + a'') \\ b(a' + a'') + a(b' + b'') & -b(b' + b'') + a(a' + a'') \end{pmatrix}, \\ &= \begin{pmatrix} (aa' - bb') + (aa'' - bb'') & -(ab' + ba') - (ab'' + ba'') \\ (ba' + ab') + (ba'' + ab'') & -(bb' - aa') - (bb'' - aa'') \end{pmatrix}, \end{aligned}$$

et d'autre part

$$B = \begin{pmatrix} aa' - bb' & -(ab' + ba') \\ ba' + ab' & aa' - bb' \end{pmatrix} + \begin{pmatrix} aa'' - bb'' & -(ab'' + ba'') \\ ba'' + ab'' & aa'' - bb'' \end{pmatrix}.$$

Sur les formules obtenues on voit immédiatement que $A = B$.

Nous avons donc démontré que $(\mathbb{C}, +, \times)$ possède les propriétés suivantes :

1. $(\mathbb{C}, +)$ est un groupe abélien.
2. La multiplication est associative, commutative, possède un élément neutre et toute matrice non nulle de $\mathbb{C}$ admet une matrice inverse dans $\mathbb{C}$.

3. La multiplication est distributive par rapport à l'addition
c'est-à-dire

Théorème et définition.

$(\mathbb{C}, +, \times)$ est un corps commutatif appelé **corps des nombres complexes.**

Lorsque nous n'aurons pas besoin de la matrice qui définit un nombre complexe nous noterons un tel nombre par une seule lettre, z par exemple.

REMARQUE

1. $(\mathbb{C}, +, \times)$ est un sous-anneau de l'anneau unitaire non commutatif $(\mathcal{M}_2, +, \times)$; ce sous-anneau a une structure de corps commutatif.

d) $\mathbb{R}$ considéré comme sous-corps de $\mathbb{C}$.

A tout nombre réel a on peut associer l'homothétie de $\mathcal{V}_2$ dans $\mathcal{V}_2$ définie par

$$(\forall \vec{v} \in \mathcal{V}_2) \quad f_a(\vec{v}) = a\vec{v}.$$

Pour toute base $(\vec{i}, \vec{j})$ de $\mathcal{V}_2$ on a donc $f_a(\vec{i}) = a\vec{i}$ et $f_a(\vec{j}) = a\vec{j}$; la matrice associée à f_a dans toute base est donc

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

Désignons par S l'ensemble de ces matrices, S est une partie de $\mathbb{C}$; cette partie est *stable* pour l'addition et la multiplication, car, quels que soient les réels a et a', on a

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} a' & 0 \\ 0 & a' \end{pmatrix} = \begin{pmatrix} a+a' & 0 \\ 0 & a+a' \end{pmatrix} \tag{3}$$

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} a' & 0 \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ 0 & aa' \end{pmatrix}. \tag{3'}$$

Considérons l'application φ

$$\varphi : \mathbb{R} \longrightarrow \mathbf{S}$$
$$a \longmapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

cette application est visiblement *bijective*; d'autre part les formules (3) et (3') montrent que, quels que soient les réels a et a', on a

$$\varphi(a+a') = \varphi(a) + \varphi(a')$$
$$\varphi(aa') = \varphi(a)\,\varphi(a').$$

La bijection φ définit donc un *isomorphisme* du corps commutatif $(\mathbb{R}, +, \times)$ sur $(\mathbf{S}, +, \times)$.
Donc $(\mathbf{S}, +, \times)$ est un *corps commutatif*. On conviendra d'identifier S et $\mathbb{R}$ c'est-à-dire on posera

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a$$

en particulier

$$\mathbf{O} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0 \qquad \text{et} \qquad \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

On a donc grâce à cette identification $\mathbb{R} \subset \mathbb{C}$.
Les matrices éléments de S sont appelées **matrices scalaires** d'ordre 2, nous verrons pourquoi au paragraphe suivant.

REMARQUE

2. $(S, +, \times)$ est un sous-anneau de l'anneau $(\mathcal{M}_2, +, \times)$ (cf. 4.4 d); il a une structure de corps commutatif.
D'autre part c'est un sous-corps du corps $(\mathbb{C}, +, \times)$.
Enfin $(S, +, \times)$ est isomorphe à $(\mathcal{K}, +, o)$ (cf. ex. 4 du § 4.3 d).

4. 6 $\mathbb{C}$ ESPACE VECTORIEL SUR $\mathbb{R}$

a) Multiplication externe d'un nombre complexe par un nombre réel. Espace vectoriel $\mathbb{C}$ sur $\mathbb{R}$.

A l'aide de l'identification précédente, nous pouvons calculer le produit de $\lambda \in \mathbb{R}$ par $z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathbb{C}$; nous avons

$$\lambda \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} \lambda a & -\lambda b \\ \lambda b & \lambda a \end{pmatrix}.$$

Nous définissons ainsi une application

$$\mathbb{R} \times \mathbb{C} \longrightarrow \mathbb{C},$$

opération externe dans $\mathbb{C}$, le domaine d'opérateurs étant $\mathbb{R}$. L'ensemble $\mathbb{C}$ est ainsi muni :
— d'une opération interne, l'addition, telle que $(\mathbb{C}, +)$ est un groupe abélien;
— d'une opération externe qui possède les propriétés suivantes :
Quels que soient λ et λ' de $\mathbb{R}$ et z et z' de $\mathbb{C}$, on a

$$1.\ z = z,$$
$$\lambda(\lambda' z) = (\lambda\lambda') z,$$
$$(\lambda + \lambda') z = \lambda z + \lambda' z,$$
$$\lambda(z + z') = \lambda z + \lambda z';$$

en effet comme $\mathbb{R} \subset \mathbb{C}$ ces formules ne font que traduire, dans des cas particuliers, des propriétés du corps $(\mathbb{C}, +, \times)$. Il en résulte (cf. § 4.1) :

Théorème.
L'ensemble $\mathbb{C}$ muni de l'addition des nombres complexes et de la multiplication externe d'un nombre complexe par un nombre réel est un espace vectoriel sur $\mathbb{R}$.

Dans l'espace vectoriel $\mathbb{C}$ sur $\mathbb{R}$, les « *vecteurs* » sont les nombres complexes, les « *scalaires* » sont les nombres réels; ceci explique le terme matrice scalaire attribuée à $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} = a$.

EXERCICE

1. Démontrer que z_1 et z_2 sont linéairement indépendants dans $\mathbb{C}$, espace vectoriel sur $\mathbb{R}$, si et seulement si z_1 et z_2 sont non nuls et tels que $z_1 (z_2)^{-1} \notin \mathbb{R}$.
Il en est ainsi de 1 et $z_0 \notin \mathbb{R}$.

b) Base de $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$. Dimension.

En utilisant les définitions de l'addition et de la multiplication externe indiquées précédemment, il est possible d'écrire les égalités suivantes, pour tout élément $z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ de $\mathbb{C}$:

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} 0 & -b \\ b & 0 \end{pmatrix}$$
$$= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Tout élément de $\mathbb{C}$ peut donc s'exprimer comme combinaison linéaire des deux matrices $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; la famille $\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right)$ est donc une famille *génératrice* de $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$. C'est d'autre part une famille *libre* puisque quels que soient les réels a et b

$$\left[a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right] \Longleftrightarrow (a = b = 0).$$

Cette famille est donc une *base* de l'espace vectoriel considéré, qui est, en conséquence, de *dimension* 2.

La matrice $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ a déjà été identifiée au nombre réel 1. Nous posons, d'autre part, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = i$.

Par suite, nous écrivons : $z = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a + bi$, de manière unique, puisque $(1, i)$ est une base.

EXERCICE

2. Démontrer que (z_1, z_2) où z_1 et z_2 sont non nuls et de rapport non réel est une base de $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$ (cf. ex. 1 ci-dessus).

Nous dirons que $(1, i)$ est la **base canonique** de $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$.
Quels que soient les nombres complexes

$$z = a + bi \quad , \quad z' = a' + b'i$$

On a donc, puisque $(1, i)$ est une base,

$$(z = z') \Longleftrightarrow \begin{cases} a = a', \\ \text{et} \\ b = b'. \end{cases}$$

Nous connaissions d'ailleurs déjà cette propriété grâce à l'égalité des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ et $\begin{pmatrix} a' & -b' \\ b' & b' \end{pmatrix}$.

EXERCICE

3. Étant donné un nombre complexe non réel z_0, démontrer que tout nombre complexe z peut s'écrire d'une manière unique sous la forme $z = \alpha + \beta z_0$ $(\alpha, \beta \in \mathbb{R})$ (considérer la base $(1, z_0)$ cf. ex. 2 ci-dessus).

ATTENTION. De même que $\mathbb{R}$ peut être considéré comme espace vectoriel sur lui-même, tout corps commutatif K est un espace vectoriel sur K ; l'espace vectoriel est K, le domaine d'opérateurs est K lui-même.

Donc $\mathbb{C}$ *est aussi un espace vectoriel sur* $\mathbb{C}$. Mais il faut bien remarquer que les deux objets mathématiques

- $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$
- $\mathbb{C}$ espace vectoriel sur $\mathbb{C}$

sont *deux objets distincts.* Certaines de leurs propriétés peuvent être distinctes; par exemple deux nombres complexes non nuls z_1 et z_2 tels que $z_2 = \lambda z_1$ avec $\lambda \notin \mathbb{R}$ sont linéairement *indépendants* dans $\mathbb{C}$ espace vectoriel sur $\mathbb{R}$ (cf. ex. 1 ci-dessus), en revanche ils sont *linéairement dépendants* dans $\mathbb{C}$ espace vectoriel sur $\mathbb{C}$.

Si z_0 est un nombre complexe non nul (z_0) est une base de $\mathbb{C}$ espace vectoriel sur $\mathbb{C}$; en effet tout nombre complexe z peut s'écrire d'une manière unique $z = \lambda z_0$ avec $\lambda \in \mathbb{C}$ (on a $\lambda = z(z_0)^{-1}$); avec des notations évidentes nous écrirons

$$\dim_{\mathbb{C}} \mathbb{C} = 1 \qquad \dim_{\mathbb{R}} \mathbb{C} = 2.$$

On voit que dans le terme « E espace vectoriel sur K » la locution « sur K » est essentielle; on ne l'omet que s'il n'y a aucune ambiguïté sur le domaine des opérateurs considéré dans la question.

4. 7 DÉFINITIONS ET NOTATIONS DIVERSES. RÈGLES DE CALCUL DANS $\mathbb{C}$

a) Introduction. Définitions et notations diverses.

Calculons i^2 on a

$$i^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -1$$

$$\boxed{i^2 = -1}.$$

REMARQUE

1. Lorsque l'on a inventé les nombres complexes (en Italie au XVI^e siècle) on ne connaissait que les nombres réels qui sont tels que pour tout x on ait $x^2 \geqslant 0$; donc les « nombres » tels que $x^2 < 0$ « n'existaient pas » ce qui a entraîné pour les nouveaux nombres inventés — où en particulier $i^2 = -1$ » l'appelation de « *nombres imaginaires* ». Les éléments de $\mathbb{C}$ « existant » tout comme les éléments de $\mathbb{R}$, on a abandonné plus tard le terme de nombre imaginaire pour celui de nombre complexe. Cependant comme nous le verrons le terme « imaginaire » subsiste dans certaines définitions utilisées aujourd'hui.

Tout nombre complexe z s'écrit d'une manière unique

$$z = a + bi \qquad \text{où} \qquad a \text{ et } b \in \mathbb{R}$$

Cette forme est appelée **forme algébrique** d'un nombre complexe — par opposition avec une autre forme que nous verrons au § 4.11, la forme trigonométrique.

Le nombre réel a est appelé **partie réelle** de $z = a + bi$,
le nombre réel b est appelé **partie imaginaire** de $z = a + bi$.
On pose

$$a = \Re(z) \qquad \text{et} \qquad b = \Im(z).$$

Naturellement le terme « *partie imaginaire* » pour b *réel* est un abus de langage; on peut dire également — ce qui serait plus correct — que b est le « coefficient de i » dans $z = a + bi$.

Les nombres complexes de la forme bi où $b \in \mathbb{R}$ sont appelés **nombres imaginaires purs.**

Leur ensemble se notera $i\,\mathbb{R}$; $i\,\mathbb{R}$ est stable pour l'addition, c'est même un sous-groupe de $(\mathbb{C}, +)$; en revanche $i\,\mathbb{R}$ n'est pas stable pour la multiplication puisqu'en particulier $i^2 = -1 \in \mathbb{R}$.

Le nombre complexe $a - bi$ noté $\bar{z}$ (« z *barre* ») est appelé **complexe conjugué** de $z = a + bi$. Le conjugué de $a - bi$ étant $a + bi$ on dit que z et $\bar{z}$ sont **deux nombres complexes conjugués.**

b) Règles de calcul dans $\mathbb{C}$.

Soient deux nombres complexes

$$z = a + bi, \qquad z' = a' + b'i$$

où a, b, a', b' sont des nombres réels.
On a

$$z + z' = (a + bi) + (a' + b'i) = (a + a') + (b + b')\,i$$

d'où

$$\begin{cases} \mathcal{R}(z + z') = \mathcal{R}(z) + \mathcal{R}(z') \\ \mathcal{I}(z + z') = \mathcal{I}(z) + \mathcal{I}(z') \end{cases} \quad \text{et} \quad \begin{cases} \mathcal{R}(-z) = -\mathcal{R}(z), \\ \mathcal{I}(-z) = -\mathcal{I}(z). \end{cases}$$

D'autre part la relation $i^2 = -1$ nous permet d'écrire

$$\begin{aligned} zz' &= (a + bi)(a' + b'i) = aa' + (ab' + ba')\,i + bb'i^2 \\ &= aa' - bb' + (ab' + ba')\,i \end{aligned}$$

d'où

$$\begin{cases} \mathcal{R}(zz') = \mathcal{R}(z)\,\mathcal{R}(z') - \mathcal{I}(z)\,\mathcal{I}(z'), \\ \mathcal{I}(zz') = \mathcal{R}(z)\,\mathcal{I}(z') + \mathcal{R}(z')\,\mathcal{I}(z). \end{cases}$$

En particulier

$$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 \in \mathbb{R}_+.$$

Si $z \neq 0$ on a $(a, b) \neq (0, 0)$ donc $a^2 + b^2 \neq 0$; d'où dans ce cas

$$\frac{1}{z} = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}\,i.$$

On voit que les calculs dans $\mathbb{C}$, sur les nombres complexes, écrits sous la forme $a + bi$ $(a, b \in \mathbb{R})$, s'effectuent en utilisant les règles de calcul valables dans un corps commutatif et en remplaçant i^2 par -1.

EXERCICE

1. Calculer (c'est-à-dire mettre sous la forme $a + bi$, $a, b \in \mathbb{R}$) les nombres suivants $\dfrac{1}{-3 + 4i}$, $\dfrac{7 - 3i}{8 + i}$.

REMARQUE

2. Si on désigne par $(\mathbb{R} \times \mathbb{R}, +, \times)$ le produit cartésien $\mathbb{R} \times \mathbb{R}$ muni de l'addition et de la multiplication suivante

$$(a, b) + (a', b') = (a + a', b + b')$$
$$(a, b)(a', b') = (aa' - bb', ab' + ba')$$

on voit immédiatement que l'application

$$\varphi : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{C}$$
$$(a, b) \longmapsto a + bi$$

est un isomorphisme de $(\mathbb{R} \times \mathbb{R}, +, \times)$ sur $(\mathbb{C}, +, \times)$. C'est une présentation des nombres complexes souvent utilisée; elle est un peu abrupte quant à l'introduction du produit. Grâce au produit des matrices la définition du produit s'introduit plus naturellement.

c) Propriétés des nombres complexes conjugués.

Considérons l'application

$$f : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto \bar{z}$$

c'est-à-dire, a et b étant réels

$$f(a + bi) = a - bi.$$

Il est évident que cette application est *bijective*; d'autre part nous avons déjà vu que quel que soit $z = a + bi$

$$\overline{(z)} = \overline{(a - bi)} = a + bi = z$$

cette application est donc une *bijection involutive* puisqu'on a $f \circ f = \mathrm{Id}_{\mathbb{C}}$ (ou $f^{-1} = f$). D'autre part quels que soient z et z' de $\mathbb{C}$ on a

$$\overline{z + z'} = \overline{(a + bi) + (a' + b'i)} = \overline{a + a' + (b + b')i} = (a + a') - (b + b')i$$
$$= (a - bi) + (a' - b'i) = \bar{z} + \bar{z'};$$

de plus calculons $\overline{zz'}$ et $\bar{z}\,\bar{z'}$; on a

$$\overline{zz'} = \overline{(a + bi)(a' + b'i)} = \overline{aa' - bb' + (ab' + ba')i} = aa' - bb' - (ab' + ba')i$$
$$\bar{z}\,\bar{z'} = (a - bi)(a' - b'i) = aa' - bb' - (ab' + ba')i$$

donc $\overline{zz'} = \bar{z}\,\bar{z'}$.

Par conséquent quels que soient z et z' de $\mathbb{C}$

$$f(z + z') = f(z) + f(z')$$
$$f(zz') = f(z)f(z')$$

Théorème.

L'application

$$f : \mathbb{C} \longrightarrow \mathbb{C}$$
$$z \longmapsto \bar{z}$$

est un isomorphisme involutif du corps $\mathbb{C}$ sur lui-même.

Si $z = a + ib$ on voit que l'on a $z + \bar{z} = 2a$ et $z - \bar{z} = 2bi$ c'est-à-dire

$$\boxed{\mathcal{R}(z) = \frac{1}{2}(z + \bar{z}) \qquad \mathfrak{I}(z) = \frac{1}{2i}(z - \bar{z})}.$$

On en déduit les propriétés suivantes :

Quel que soit z de $\mathbb{C}$:

z est réel si et seulement si $\bar{z} = z$

z est imaginaire pur si et seulement si $\bar{z} = -z$.

La première de ces propriétés est souvent commode pour reconnaître que $z \in \mathbb{R}$.

d) Remarque sur les ordres possibles définis sur $\mathbb{C}$.

L'*ensemble* $\mathbb{C}$ peut être muni d'une relation d'ordre de bien des manières; en voici deux :

EXERCICES

Soit $z = a + bi$ et $z = a' + b'i$ $(a, b, a', b' \in \mathbb{R})$.

2. Démontrer que la relation $z \mathcal{R}_1 z'$ définie par

$$(a \leqslant a' \quad \text{et} \quad b \leqslant b')$$

est une relation d'ordre partiel défini sur $\mathbb{C}$.

3. Démontrer que la relation $z \mathcal{R}_2 z'$ définie sur $\mathbb{C}$ par

$$[a < a' \quad \text{ou} \quad (a = a' \quad \text{et} \quad b \leqslant b')]$$

est une relation d'ordre total définie sur $\mathbb{C}$.

En revanche nous allons voir qu'*il n'existe pas* dans $\mathbb{C}$ de *relation d'ordre total compatible avec l'addition et la multiplication.* Si une telle relation $\leqslant$ existait, on démontrerait comme dans $\mathbb{R}$ (cf. § 3.6) que pour tout $z \neq 0$ de $\mathbb{C}$ on a $0 < z^2$. Or $1^2 = 1$ et $i^2 = -1$ et pour une telle relation on aurait $0 < 1^2$ et $0 < i^2$, c'est-à-dire $0 < 1$ et $0 < -1$ ce qui est impossible (cf. § 3.6.*b* corollaire, où l'on remplacera $\mathbb{R}$ par $\mathbb{C}$).
Il n'existe donc pas dans $\mathbb{C}$ *de relation d'ordre total telle que* $(\mathbb{C}, +, \times, \leqslant)$ *soit un corps totalement ordonné.* C'est pour cette raison que l'on ne munit pas $\mathbb{C}$ d'un ordre; avec un tel ordre on ne pourrait pas faire de calcul mettant en jeu à la fois les opérations et l'ordre.

4. 8 REPRÉSENTATION GÉOMÉTRIQUE D'UN NOMBRE COMPLEXE

a) Plan vectoriel euclidien $\mathcal{E}_2$ (révision).

Soit deux vecteurs quelconques $\vec{v}$ et $\vec{v'}$ de $\mathcal{V}_2$ plan vectoriel sur $\mathbb{R}$; le **produit scalaire** des deux vecteurs $\vec{v}$ et $\vec{v'}$, noté $\vec{v}.\vec{v'}$ est tel que l'application

$$\begin{aligned} f : \mathcal{V}_2 \times \mathcal{V}_2 &\longrightarrow \mathbb{R} \\ (\vec{v}, \vec{v'}) &\longmapsto \vec{v}.\vec{v'} \end{aligned}$$

possède les propriétés suivantes : quels que soient les vecteurs $\vec{v}, \vec{v'}, \vec{v_1}, \vec{v_2}, \vec{v_1'}, \vec{v_2'}$ de $\mathcal{V}_2$ et quel que soit le réel λ on a

(1) $$\vec{v}.\vec{v'} = \vec{v'}.\vec{v}$$

$$\begin{cases} (2) \quad (\vec{v_1} + \vec{v_2}).\vec{v'} = \vec{v_1}.\vec{v'} + \vec{v_2}.\vec{v'} & (3) \quad \vec{v}.(\vec{v_1'} + \vec{v_2'}) = \vec{v}.\vec{v_1'} + \vec{v}.\vec{v_2'} \\ (2') \quad (\lambda \vec{v}).\vec{v'} = \lambda(\vec{v}.\vec{v'}) & (3') \quad \vec{v}.(\lambda \vec{v'}) = \lambda(\vec{v}.\vec{v'}) \end{cases}$$

(4) $$(\vec{v} \neq \vec{0}) \Longleftrightarrow (\vec{v})^2 > 0.$$

On exprime les propriétés (1) à (3') en disant que f est une **forme bilinéaire symétrique**, symétrique à cause de (1), **bi**linéaire car les applications partielles

$$\begin{array}{ccc} \mathcal{U}_2 & \longrightarrow & \mathbb{R} \\ \vec{v} & \longmapsto & \vec{v}.\vec{v'} \\ (\vec{v'} \text{ fixé}) & & \end{array} \qquad \begin{array}{ccc} \mathcal{U}_2 & \longrightarrow & \mathbb{R} \\ \vec{v'} & \longmapsto & \vec{v}.\vec{v'} \\ (\vec{v} \text{ fixé}) & & \end{array}$$

sont des applications linéaires de $\mathcal{U}_2$ dans $\mathbb{R}$.

Tout plan vectoriel $\mathcal{U}_2$ muni d'un produit scalaire est appelé **plan vectoriel euclidien**; nous l'avons noté $\mathcal{E}_2$.

Le nombre réel $(\vec{v})^2 = \vec{v}.\vec{v}$ est appelé **carré scalaire** de $\vec{v}$. L'application

$$\begin{array}{ccc} \mathcal{E}_2 & \longrightarrow & \mathbb{R}_+ \\ \vec{v} & \longmapsto & \|\vec{v}\| = \sqrt{(\vec{v})^2} \end{array}$$

possède les propriétés suivantes : quels que soient $\vec{v}$ et $\vec{v'}$ de $\mathcal{E}_2$ et λ de $\mathbb{R}$, on a

$$\|\vec{v}\| = 0 \iff \vec{v} = \vec{0}$$
$$\|\lambda \vec{v}\| = |\lambda| \, \|\vec{v}\|$$
$$\|\vec{v_1} + \vec{v_2}\| \leqslant \|\vec{v_1}\| + \|\vec{v_2}\|$$

Ce nombre $\|\vec{v}\|$ est appelé **norme euclidienne** de v.

Rappelons aussi que deux vecteurs $\vec{v}$ et $\vec{v'}$ de $\mathcal{E}_2$ sont appelés **orthogonaux** si et seulement si $\vec{v}.\vec{v'} = 0$ et qu'un vecteur $\vec{v}$ est appelé **unitaire** si et seulement si $\|\vec{v}\| = 1$.

Rappelons enfin qu'il existe dans $\mathcal{E}_2$ des bases $\{\vec{i}, \vec{j}\}$ telles que

$$\vec{i}.\vec{j} = 0 \qquad \|\vec{i}\| = \|\vec{j}\| = 1$$

elles sont appelées bases **orthonormées** de $\mathcal{E}_2$. Dans une telle base si $\vec{v} = x\vec{i} + y\vec{j}$ et $\vec{v'} = x'\vec{i} + y'\vec{j}$ on a

$$\boxed{\begin{array}{l} \vec{v} \,.\, \vec{v'} = xx' + yy' \\ \|\vec{v}\| = \sqrt{x^2 + y^2} \end{array}}$$

b) Plan affine euclidien E_2 (révision).

Rappelons qu'un **plan affine** associé au plan vectoriel $\mathcal{U}_2$ est un ensemble P de points tel qu'à tout couple $(A, B) \in P \times P$ on associe un vecteur $\vec{v}$ de $\mathcal{U}_2$ noté $\overrightarrow{AB}$ de manière que les propriétés suivantes soient vérifiées :

i. Quels que soient A, B, C de P on a

$$\overrightarrow{AB} + \overrightarrow{BC} = \overrightarrow{AC}.$$

ii. Quels que soient A de P et $\vec{v}$ de $\mathcal{U}_2$ il existe un point unique M de P tel que $\overrightarrow{AM} = \vec{v}$.

Si $(\vec{i}, \vec{j})$ est une base de $\mathcal{U}_2$ et O un point de P, $(O, \vec{i}, \vec{j})$ est un **repère** de P. Si $\overrightarrow{OM} = x\vec{i} + y\vec{j}$ on dit que x et y sont les coordonnées du point M dans le repère $(O, \vec{i}, \vec{j})$.

On appelle **plan euclidien** et on note E_2 tout plan affine associé à un plan vectoriel euclidien.

L'application

$$d : E_2 \times E_2 \longrightarrow \mathbb{R}_+$$
$$(A, B) \longmapsto \left\| \overrightarrow{AB} \right\|$$

est une **distance** définie sur E_2 c'est-à-dire

i. Quels que soient A et B de E_2 $\quad (d(A, B) = 0) \iff (A = B).$

ii. Quels que soient A, B, C de E_2 $\quad d(A, B) = d(B, A).$

iii. Quels que soient A, B, C de E_2 $\quad d(A, B) \leqslant d(A, C) + d(C, B).$

De plus cette distance est invariante pour toute translation de E_2.
On dit que $d(A, B)$ est la **distance euclidienne** des points A et B de E_2.
Si $(\vec{i}, \vec{j})$ est une base orthonormée de $\mathcal{E}_2$ on dit que $(O, \vec{i}, \vec{j})$ est un **repère orthonormé** de E_2.

c) Représentations géométriques d'un nombre complexe.

Soit $\mathcal{E}_2$ le *plan vectoriel* euclidien rapporté à la base orthonormée $(\vec{u}, \vec{v})$ et E_2 le plan euclidien associé à $\mathcal{E}_2$ rapporté au repère orthonormé $(O, \vec{u}, \vec{v})$; les deux applications

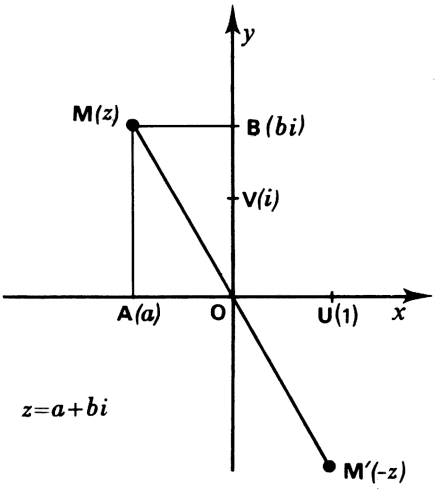
$$\begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathcal{E}_2 \\ z = a + bi & \longmapsto & \vec{V} = a\vec{u} + b\vec{v} \end{array} \qquad \begin{array}{ccc} \mathbb{C} & \longrightarrow & E_2 \\ z = a + bi & \longmapsto & M \\ (\text{où } \overrightarrow{OM} = a\vec{u} + b\vec{v}) & & \end{array}$$

sont de manière évidente des bijections.

On dit que $\vec{V} = a\vec{u} + b\vec{v}$ est le **vecteur image** du nombre complexe $z = a + bi\,(a, b \in \mathbb{R})$ dans le plan vectoriel euclidien $\mathcal{E}_2$ rapporté à la base orthonormée $(\vec{u}, \vec{v})$. On dit aussi que le point M tel que $\overrightarrow{OM} = a\vec{u} + b\vec{v}$ est le **point-image** ou tout simplement l'**image** du nombre complexe $z = a + bi$ dans le plan euclidien E_2 rapporté au repère orthonormé $(O, \vec{u}, \vec{v})$.

Réciproquement, on dit que le nombre complexe $z = a + bi$ est l'**affixe** du vecteur $\vec{V}$ ou du point M.
Dans le plan euclidien on représentera l'affixe z de M en indiquant (z) à droite du point M (fig. 1).

fig. 1



L'opposé $-z$ de z sera représenté par $-\vec{V}$ ou par M′ tel que $\overrightarrow{OM'} = -\overrightarrow{OM}$; *les points-images de z et $-z$ sont donc symétriques par rapport à* O.

Le plan E_2 utilisé pour représenter les nombres complexes est appelé quelquesfois *plan complexe*; de même on dit aussi que l'axe des abscisses est l'*axe réel* et l'axe des ordonnées l'*axe imaginaire*; ce sont évidemment des abus de langage.

Soit deux nombres complexes z et z' d'images respectives M et M′ :

$z = a + bi$ a pour vecteur image $\vec{V} = \overrightarrow{OM} = a\vec{u} + b\vec{v}$,

$z' = a' + b'i$ a pour vecteur image $\vec{V'} = \overrightarrow{OM'} = a'\vec{u} + b'\vec{v}$;

donc $z + z'$ a pour vecteur image

$$(a + a')\vec{u} + (b + b')\vec{v} = \vec{V} + \vec{V'} = \overrightarrow{OS}$$

et le point S est l'image de $z + z'$ (fig. 2).

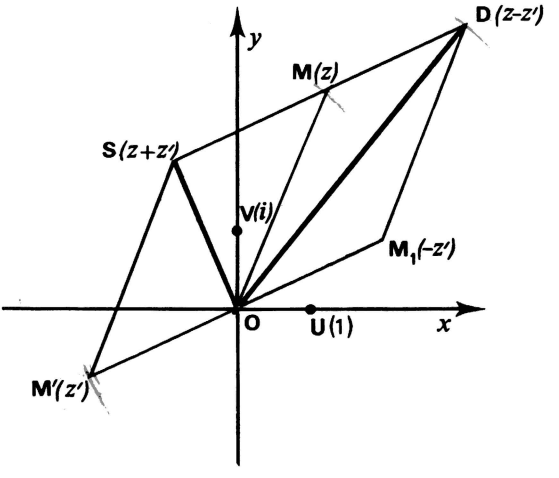


fig. 2

Il en résulte que $z - z'$ a pour vecteur image $\vec{V} - \vec{V'}$ (fig. 2); c'est-à-dire si M_1 est l'image de $(-z')$ et D celle de $z - z'$ on a

$$\overrightarrow{OD} = \vec{V} - \vec{V'} = \overrightarrow{OM} + \overrightarrow{OM_1} = \overrightarrow{OM} - \overrightarrow{OM'} = \overrightarrow{M'M}$$

d'où

L'affixe du vecteur $\overrightarrow{M'M}$ est égale à l'affixe de M diminuée de l'affixe de M′.

REMARQUES

1. La représentation d'un nombre complexe pourrait se faire par un vecteur $\vec{V}$ d'un plan vectoriel $\mathcal{V}_2$ ou par un point M d'un plan affine sans supposer qu'ils sont euclidiens. Pour interpréter simplement les nombres complexes conjugués et surtout le produit de deux nombres complexes nous aurons besoin en revanche d'utiliser un plan vectoriel euclidien $\mathcal{E}_2$ et un plan euclidien E_2; c'est pour cette raison que, traditionnellement, on représente dès le début les nombres complexes par des éléments de $\mathcal{E}_2$ et de E_2.
2. Si le nombre complexe z est réel l'affixe est l'*abscisse* de M image de z sur l'axe réel $(O, \vec{u})$ et l'affixe de $\overrightarrow{M'M}$ est $\overline{M'M}$; le résultat obtenu sur $z' - z$ se réduit alors a un résultat bien connu $\overline{M'M} = \overline{OM} - \overline{OM'}$.

EXERCICES

1. Démontrer que $(\mathbb{C}, +)$ est isomorphe à $(\mathcal{V}_2, +)$.
2. Soit a l'affixe d'un vecteur $\vec{A}$ donné; soient deux nombres complexes z et z', d'images respectives M et M′, tels que
$$z' = z + a.$$
Comment M′ se déduit-il de M?
Désignant par $\mathcal{T}$ l'ensemble des translations du plan, démontrer que $(\mathbb{C}, +)$ est isomorphe à $(\mathcal{T}, o)$.
3. Soit z l'affixe d'un point M dans le repère $(O, \vec{u}, \vec{v})$ et Z l'affixe du même point M dans le repère $(O', \vec{u}, \vec{v})$. On donne l'affixe $a + bi$ du vecteur $\overrightarrow{OO'}$. Quelle relation existe-t-il entre z, Z et $a + bi$?

Considérons enfin les images dans le plan euclidien E_2 de deux nombres complexes conjugués, nous trouvons les propriétés suivantes, z et $\bar{z}$ ayant pour images respectives M et M′ (fig. 3) :

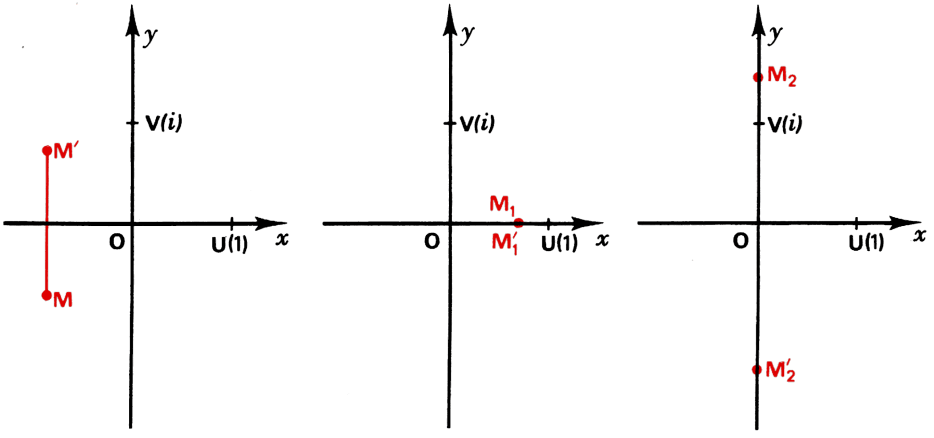


fig. 3

— le point M′ est le symétrique du point M par rapport à la droite D $(O, \vec{u})$;
— si z est réel, M et M′ sont confondus (points M_1, M'_1);
— si z est imaginaire pur, M et M′ sont symétriques par rapport au point O (points M_2, M'_2).

4. 9 MODULE D'UN NOMBRE COMPLEXE. APPLICATIONS

a) Définition et propriétés du module d'un nombre complexe.

Quel que soit le nombre complexe $z = a + bi$ on a
$$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2.$$
Ce nombre réel $a^2 + b^2$ est positif; le nombre réel positif $\sqrt{z\bar{z}}$ est appelé **module** de z.

Si z est réel, $z = a$; son module n'est autre que $\sqrt{a^2} = |a|$; nous noterons également $|z|$ le module de z; donc pour tout z de C

$$\boxed{|z| = \sqrt{z\bar{z}}}.$$

Remarquons que l'on a, quel que soit z,

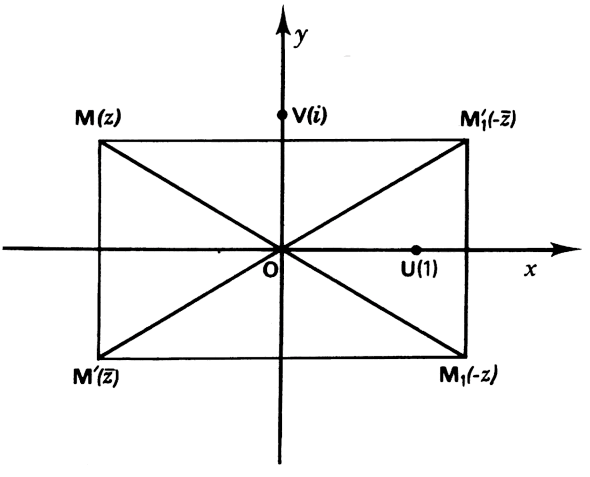
$$|z| = |-z| = |\bar{z}| = |-\bar{z}|.$$

Si M est l'image de z dans le plan euclidien E_2, voit que $|z|$ est la distance $d(O, M)$ ou la norme euclidienne de $\overrightarrow{OM}$

$$|z| = d(O, M) = \|\overrightarrow{OM}\|.$$

On a représenté sur la figure 4 les images de z, $-z$, $\bar{z}$ et $-\bar{z}$, ces images définissent un rectangle.

Fig. 4



D'autre part, quel que soit $z = a + ib$, nous avons

$$a \leqslant |a| \leqslant \sqrt{a^2 + b^2}, \qquad b \leqslant |b| \leqslant \sqrt{a^2 + b^2}$$

donc

$$\Re(z) \leqslant |z| \qquad \text{et} \qquad \Im(z) \leqslant |z|.$$

Considérons l'application

$$\begin{aligned} v : \mathbb{C} &\longrightarrow \mathbb{R}_+ \\ z &\longmapsto |z|. \end{aligned}$$

Quel que soit $z = a + bi$, $|z| = 0$ est équivalent à $a^2 + b^2 = 0$ c'est-à-dire à $(a, b) = (0, 0)$ ou encore $z = 0$.

Soient deux nombres complexes quelconques z et z'; comparons $|zz'|$ et $|z||z'|$; comme ces nombres sont des réels positifs il suffit de comparer leurs carrés. La définition du module et les propriétés du produit nous permettent d'écrire

$$|zz'|^2 = (zz')(\bar{z}\bar{z}') = (zz')(\bar{z}\bar{z}') = (z\bar{z})(z'\bar{z}') = |z|^2 |z'|^2$$

donc

$$|zz'| = |z| \times |z'|.$$

Calculons de même $|z+z'|$; nous avons

$$|z+z'|^2=(z+z')(\overline{z+z'})=(z+z')(\overline{z}+\overline{z'})$$
$$=z\overline{z}+(z\overline{z'}+z'\overline{z})+z'\overline{z'}=|z|^2+(z\overline{z'}+z'\overline{z})+|z'|^2.$$

Or $z\overline{z'}$ et $\overline{z}z'$ sont conjugués donc

$$z\overline{z'}+z'\overline{z}=2\mathcal{R}(z\overline{z'})\leqslant 2|z\overline{z'}|=2|z|\times|\overline{z'}|=2|z|\times|z'|$$

et par conséquent

$$|z+z'|^2\leqslant|z|^2+2|z|\times|z'|+|z'|^2=(|z|+|z'|)^2$$

d'où

$$|z+z'|\leqslant|z|+|z'|.$$

REMARQUE

1. Nous avons tenu à donner cette démonstration à titre d'exercice sur les nombres conjugués et les modules. En fait $|z|$ étant la norme euclidienne de $\overrightarrow{OM}$ on a immédiatement

$$|z+z'|=\|\overrightarrow{OM}+\overrightarrow{OM'}\|\leqslant\|\overrightarrow{OM}\|+\|\overrightarrow{OM'}\|=|z|+|z'|.$$

Concluons :

Théorème.

L'application

$$v:\mathbb{C}\longrightarrow\mathbb{R}_+,\quad z\longmapsto|z|$$

possède les propriétés suivantes :

V_1. Quel que soit z de $\mathbb{C}$

$$(z=0)\iff(|z|=0).$$

V_2. Quels que soient z et z' de $\mathbb{C}$

$$|zz'|=|z|\times|z'|.$$

V_3. Quels que soient z et z' de $\mathbb{C}$

$$|z+z'|\leqslant|z|+|z'|.$$

L'application v a donc les mêmes propriétés que l'application de $\mathbb{R}$ dans $\mathbb{R}_+$ qui à tout x de $\mathbb{R}$ associe $|x|$; nous dirons encore, dans $\mathbb{C}$, que $|z|$ définit une **valeur absolue.**

b) Distance définie sur $\mathbb{C}$.

Comme dans $\mathbb{R}$ (cf. § 3.8) on obtient les résultats suivants :

Corollaire.

L'application

$$d:\mathbb{C}\times\mathbb{C}\longrightarrow\mathbb{R}_+,\quad (z,z')\longmapsto|z-z'|$$

possède les propriétés suivantes :

D_1. Quels que soient z et z' de $\mathbb{C}$

$$d(z,z')=0)\iff(z=z').$$

D_2. Quels que soient z et z' de $\mathbb{C}$

$$d(z,z')=d(z',z).$$

D. Quels que soient z, z', z'' de $\mathbb{C}$

$$d(z,z')\leqslant d(z,z'')+d(z'',z').$$

Autrement dit, d est une **distance** définie sur $\mathbb{C}$ et par conséquent $(\mathbb{C}, d)$ est un **espace métrique.**

D'ailleurs si M et M′ sont les images respectives de z et z' dans E_2 on a

$$d(z, z') = |z - z'| = \|\overrightarrow{MM'}\| = d(M, M').$$

EXERCICES

1. Démontrer par récurrence que l'on a

$$\left|\sum_{k=1}^{k=n} z_k\right| \leqslant \sum_{k=1}^{k=n} |z_k|.$$

2. Démontrer que quels que soient z et z' de $\mathbb{C}$ on a

$$\big||z| - |z'|\big| \leqslant |z + z'|.$$

3. Comment faut-il choisir z et z' pour que l'on ait

$$|z + z'| = |z| + |z'|? \qquad |z + z'| = \big||z| - |z'|\big|?$$

REMARQUE

2. Puisque $|-z'| = |z'|$ et $z - z' = z + (-z')$ on a aussi, quels que soient z et z' de $\mathbb{C}$,

$$\big||z| - |z'|\big| \leqslant |z - z'| \leqslant |z| + |z'|.$$

c) Application aux calculs dans $\mathbb{C}$ (multiplication et division).

On démontrera facilement par récurrence que l'on a

$$\left|\prod_{k=1}^{k=n} z_k\right| = \prod_{k=1}^{k=n} |z_k|.$$

Soit maintenant $z = a + bi$ un nombre complexe **non nul** et z^{-1} son inverse; la relation $zz^{-1} = 1$ est équivalente à $(zz^{-1})\,\bar{z} = \bar{z}$ c'est-à-dire à $z^{-1}\,|z|^2 = \bar{z}$ d'où

$$\text{si } z \neq 0 \qquad z^{-1} = \frac{\bar{z}}{|z|^2}$$

ou encore

$$\text{si } a + bi \neq 0 \qquad (a + bi)^{-1} = \frac{a - bi}{a^2 + b^2},$$

formule que nous avions déjà obtenue.

Ceci nous permet d'écrire sous la forme $a + bi$ le quotient de deux nombres complexes z et z' $(z' \neq 0)$ mis sous cette forme

$$\frac{z}{z'} = zz'^{-1} = \frac{z\bar{z}'}{|z'|^2}.$$

Par exemple

$$\frac{1 - 2i}{7 + 3i} = \frac{(1 - 2i)(7 - 3i)}{49 + 9} = \frac{7 - 3i - 14i - 6}{58} = \frac{1 - 17i}{58}.$$

d) Nombres complexes de module 1.

L'ensemble des nombres complexes de module 1 est l'ensemble des nombres complexes $z = a + bi$ $(a, b \in \mathbb{R})$ où

$$|z| = \sqrt{a^2 + b^2} = 1.$$

C'est donc l'ensemble des matrices $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ où $a^2 + b^2 = 1$; nous avons désigné dans le cours de première cet ensemble de matrices par $\mathbf{O}_2^+$.

On représente aussi l'ensemble des nombres complexes de module 1 par $\mathbb{U}$.

Cet ensemble $\mathbb{U}$ n'est pas vide (il contient 1) et quels que soient z et z' de $\mathbb{U}$ on a $|z| = |z'| = 1$ d'où $|z'^{-1}| = 1$ et par conséquent

$$|zz'^{-1}| = |z| \times |z'^{-1}| = 1$$

donc $zz'^{-1} \in \mathbb{U}$ et nous pouvons énoncer (cf. § 2.6 a) :

$(\mathbb{U}, \times)$ est un sous-groupe du groupe $(\mathbb{C}^*, \times)$.

EXERCICE

4. Démontrer que, quel que soit z de $\mathbb{C}$, on a

$$(|z| = 1) \iff (\bar{z} = z^{-1}).$$

Soit z un nombre complexe **non nul** ; le nombre complexe $z_0 = \dfrac{z}{|z|}$ est entièrement déterminé, d'autre part il a pour module 1 d'où

Tout nombre complexe **non nul** z peut s'écrire d'une manière unique sous la forme

$$z = |z| z_0 \quad \text{où} \quad |z_0| = 1.$$

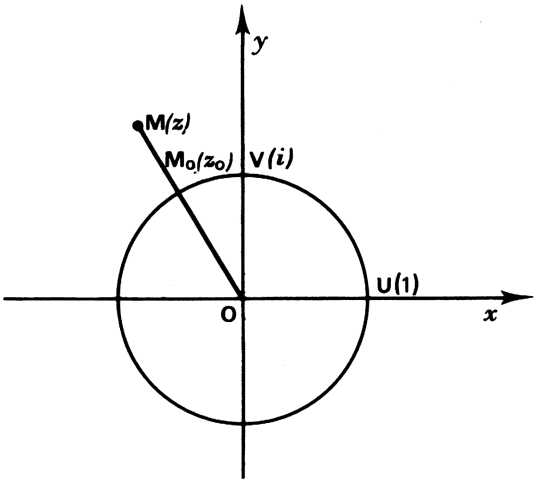


fig. 5

Géométriquement $\mathbb{U}$ est représenté par le cercle trigonométrique (cercle de centre O et de rayon 1) (fig. 5). Si M est l'image de $z \neq 0$, z_0 a pour image le point M_0 où la demi-droite [O, M) perce le cercle trigonométrique.

4. 10 RACINES CARRÉES ET ÉQUATIONS DU SECOND DEGRÉ

a) Racines carrées d'un nombre complexe.

Nous avons déjà démontré que dans $\mathbb{C}$, il existe un nombre i dont le carré est égal à -1. Ce nombre i est une racine carrée de -1.

Nous allons rechercher toutes les racines carrées d'un nombre complexe donné.

EXEMPLE

Étant donné le nombre complexe $z = 3 + 4i$, existe-t-il un nombre complexe $Z = x + iy$ tel que $Z^2 = z$?

Quel que soit Z c'est-à-dire, quels que soient x et y réels, les relations suivantes sont équivalentes (rappelons que l'accolade signifie conjonctions des propriétés ainsi réunies) :

$$(x + iy)^2 = 3 + 4i,$$
$$x^2 - y^2 + 2ixy = 3 + 4i,$$
$$\begin{cases} x^2 - y^2 = 3, \\ xy = 2, \end{cases}$$
$$\begin{cases} x^2 + (-y^2) = 3, \\ x^2(-y^2) = -4, \\ xy > 0. \end{cases}$$

Les deux nombres réels x^2 et $(-y^2)$ sont donc racines de l'équation du second degré à coefficients et inconnue réels

$$t^2 - 3t - 4 = 0.$$

Les racines de cette équation sont 4 et -1.

D'où, sans ambiguïté

$$x^2 = 4 \quad \text{et} \quad -y^2 = -1,$$

et, par suite

$$x = 2\varepsilon \quad \text{et} \quad y = \varepsilon' \text{ (avec } \varepsilon^2 = 1 \text{ et } \varepsilon'^2 = 1).$$

D'autre part, la condition $xy > 0$ doit être réalisée; elle se ramène à $\varepsilon\varepsilon' > 0$. D'où les racines cherchées

$$Z_1 = 2 + i,$$
$$Z_2 = -2 - i.$$

Étude du cas général.

Donnons-nous $z = a + bi$ $(a, b \in \mathbb{R})$ et cherchons Z de $\mathbb{C}$ tel que $Z^2 = z$. Posons $Z = x + iy$ $(x, y \in \mathbb{R})$; quels que soient x, y, a, b de $\mathbb{R}$ les relations suivantes sont équivalentes :

$$(x + iy)^2 = a + bi$$
$$x^2 - y^2 + 2ixy = a + bi$$
$$\begin{cases} x^2 - y^2 = a \\ 2xy = b \end{cases}$$
$$\begin{cases} x^2 + (-y^2) = a & (1) \\ x^2(-y^2) = -\dfrac{b^2}{4} & (2) \\ xyb \geqslant 0 & (3) \end{cases}$$

Les deux nombres x^2 et $-y^2$ sont donc racines de l'équation :

$$t^2 - at - \frac{b^2}{4} = 0 \qquad (4)$$

où les coefficients et l'inconnue sont réels.

Premier cas : $a = b = 0$ (c'est-à-dire $z = 0$).

L'équation (4) se réduit à :

$$t^2 = 0;$$

d'où $x^2 = 0$, $y^2 = 0$, et le nombre complexe cherché est 0.

Deuxième cas : $a \neq 0$ et $b = 0$ (c'est-à-dire $z \in \mathbb{R}$).

L'équation (4) devient :

$$t^2 - at = 0;$$

ses racines sont 0 et a.

- **Si $a > 0$**, il est obligatoire que l'on ait :

$$x^2 = a, \quad -y^2 = 0,$$

soit $x = \varepsilon\sqrt{a}$, $y = 0$ (avec $\varepsilon^2 = 1$).
La condition (3) est réalisée.
Le nombre $z = a$ admet donc deux racines carrées Z_1 et Z_2 qui sont

$$Z_1 = \sqrt{a} \quad \text{et} \quad Z_2 = -\sqrt{a}.$$

Un nombre réel positif admet donc, dans $\mathbb{C}$, les mêmes racines carrées que dans $\mathbb{R}$.

- **Si $a < 0$,** x et y vérifient :

$$x^2 = 0, \quad -y^2 = a,$$

d'où $x = 0$, $y = \varepsilon\sqrt{-a}$ (avec $\varepsilon^2 = 1$).
La condition (3) est réalisée.
Le nombre réel négatif $z = a$ admet donc deux racines carrées Z_1 et Z_2 qui sont :

$$Z_1 = i\sqrt{-a} \quad \text{et} \quad Z_2 = -i\sqrt{-a}.$$

Troisième cas : $b \neq 0$ (c'est-à-dire $z \notin \mathbb{R}$).

L'équation (4) admet deux racines de signes contraires, donc, sans ambiguïté :

$$x^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \quad \text{et} \quad -y^2 = \frac{a - \sqrt{a^2 + b^2}}{2}$$

soit :

$$x = \varepsilon\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} \quad \text{et} \quad y = \varepsilon'\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}},$$

avec : $\varepsilon^2 = 1$ et $\varepsilon'^2 = 1$.
La condition (3) est réalisée si et seulement si $\varepsilon\varepsilon' b \geqslant 0$, ce qui exige que le produit $\varepsilon\varepsilon'$ soit toujours du signe de b (puisque $b \neq 0$).
Si l'on *choisit* deux valeurs ε_1 et ε'_1 de ε et ε' qui conviennent, les valeurs opposées conviennent aussi, et ce sont les seules. Le nombre z admet encore deux racines carrées qui sont :

$$Z_1 = \varepsilon_1\sqrt{\frac{a_1 + \sqrt{a^2 + b^2}}{2}} + \varepsilon'_1 i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}},$$

$$Z_2 = -\varepsilon_1\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} - \varepsilon'_1 i\sqrt{\frac{-a + \sqrt{a^2 + b^2}}{2}}.$$

Ces deux racines carrées sont opposées.

Théorème.

Tout nombre complexe non nul admet deux racines carrées distinctes et opposées.

EXERCICE

1. Déterminer les racines carrées des nombres complexes suivants :

$$-1, \quad 2i, \quad 4-3i, \quad 1+i.$$

b) Résolution d'une équation du second degré.

Soit l'équation :

$$ax^2 + bx + c = 0,$$

où a, b, c sont des nombres réels ou complexes ($a \neq 0$), et où x représente l'inconnue complexe.

Cette équation a les mêmes solutions que les équations suivantes :

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0,$$

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}.$$

Premier cas. Supposons a, b, c réels.

Si $b^2 - 4ac > 0$, le nombre $\dfrac{b^2 - 4ac}{4a^2}$ admet deux racines carrées qui sont égales à :

$$\frac{\varepsilon\sqrt{b^2 - 4ac}}{2} \quad (\text{avec} \quad \varepsilon^2 = 1).$$

L'équation donnée admet donc *deux racines réelles distinctes* qui sont :

$$x' = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{et} \quad x'' = \frac{-b - \sqrt{b^2 - 4ac}}{2a}.$$

Si $b^2 - 4ac = 0$, l'équation se réduit à

$$\left(x + \frac{b}{2a}\right)^2 = 0.$$

Elle admet une *racine double réelle*, égale à $-\dfrac{b}{2a}$.

Si $b^2 - 4ac < 0$, le nombre $\dfrac{b^2 - 4ac}{4a^2}$ admet deux racines carrées qui sont égales à $\varepsilon i\dfrac{\sqrt{4ac - b^2}}{2a}$ et l'équation donnée admet deux solutions qui sont les nombres *complexes conjugués distincts*

$$x' = \frac{-b + i\sqrt{4ac - b^2}}{2a} \quad \text{et} \quad x'' = \frac{-b - i\sqrt{4ac - b^2}}{2a}.$$

On remarquera que le nombre réel sous le radical est $4ac - b^2 > 0$ et non $b^2 - 4ac$ qui, lui, est strictement négatif. Concluons

---

Toute équation $ax^2 + bx + c$ à **coefficients réels** ($a \neq 0$) admet deux solutions

si $b^2 - 4ac > 0$ ces solutions sont réelles et distinctes,
si $b^2 - 4ac = 0$ ces solutions sont réelles et confondues,
si $b^2 - 4ac < 0$ ces solutions sont des nombres complexes conjugués distincts.

Deuxième cas. Supposons a, b, c complexes.

Si $b^2 - 4ac \neq 0$, le nombre complexe $b^2 - 4ac$ admet deux racines carrées opposées distinctes z_1 et $-z_1$. L'équation a donc deux solutions distinctes

$$x' = \frac{-b + z_1}{2a} \qquad \text{et} \qquad x'' = \frac{-b - z_1}{2a}.$$

Si $b^2 - 4ac = 0$, l'équation admet deux solutions confondues

$$x' = x'' = -\frac{b}{2a}.$$

Concluons :

Toute équation $ax^2 + bx + c = 0$ à **coefficients complexes** ($a \neq 0$) admet deux solutions dans $\mathbb{C}$
si $b^2 - 4ac \neq 0$ ces solutions sont distinctes,
si $b^2 - 4ac = 0$ ces solutions sont confondues.

On remarquera la **différence entre ces deux discussions**
si a, b, c sont **réels** 3 cas $b^2 - 4ac > 0$,
$b^2 - 4ac = 0$,
$b^2 - 4ac < 0$,

et si a, b, c sont **complexes** 2 cas seulement $b^2 - 4ac \neq 0$,
$b^2 - 4ac = 0$.

EXERCICES

Résoudre dans $\mathbb{C}$ les équations suivantes :

2. $x^2 + x + 1 = 0$,
3. $x^2 - x + 2 = 0$,
4. $x^2 - (5 - 14i)x - 2(5i + 12) = 0$.

III. Argument d'un nombre complexe. Applications

4. 11 ROTATIONS ET ANGLES DU PLAN VECTORIEL EUCLIDIEN $\mathcal{E}_2$ (REVISION)

a) Isométries de $\mathcal{E}_2$.

On appelle **isométrie vectorielle** de $\mathcal{E}_2$ toute *application linéaire* de $\mathcal{E}_2$ dans $\mathcal{E}_2$ qui *conserve la norme* de tout vecteur de $\mathcal{E}_2$.
Ainsi f élément de $\mathcal{L}(\mathcal{E}_2)$ est une isométrie vectorielle si et seulement si

$$(\forall \vec{v} \in \mathcal{E}_2) \quad \|f(\vec{v})\| = \|\vec{v}\|.$$

On voit immédiatement qu'une isométrie de $\mathcal{E}_2$ est un *isomorphisme* de $\mathcal{E}_2$ sur $\mathcal{E}_2$; en effet, d'après les propriétés de la norme, $f(\vec{v}) = \vec{0}$ est équivalent à $\|f(\vec{v})\| = \|\vec{v}\| = 0$, c'est-à-dire à $\vec{v} = \vec{0}$; donc le noyau de f est $\{\vec{0}\}$ et par conséquent f est un isomorphisme de $\mathcal{E}_2$ sur $\mathcal{E}_2$ (cf. § 4.4 c).

D'autre part les relations

$$\left\|\vec{v}\right\| = \sqrt{\vec{v}.\vec{v}} \qquad \text{et} \qquad \vec{v}.\vec{v'} = \frac{1}{2}\left[\left\|\vec{v}+\vec{v'}\right\|^2 - \left\|\vec{v}\right\|^2 - \left\|\vec{v'}\right\|^2\right]$$

montrent que $f \in \mathfrak{L}(\mathcal{E}_2)$ est une isométrie si et seulement si *f conserve le produit scalaire*. Nous en avons déduit que $f \in \mathfrak{L}(\mathcal{E}_2)$ est une isométrie si et seulement si l'*image de toute base orthonormée par* f *est une base orthonormée*.

Nous avons enfin montré que $(\mathfrak{I}, \circ)$ est un groupe, $\mathfrak{I}$ désignant l'ensemble des isométries de $\mathcal{E}_2$.

b) Rotations de $\mathcal{E}_2$. Groupes $(\mathcal{R}, \circ)$ et $(\mathbf{O}_2^+, \times)$.

Nous avons vu que toute isométrie de $\mathcal{E}_2$ a, relativement à une base orthonormée quelconque de $\mathcal{E}_2$, une matrice qui est de l'un des deux types suivants

$$\text{(I)} \quad \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \qquad\qquad \text{(II)} \quad \begin{pmatrix} a & b \\ b & -a \end{pmatrix}$$

avec dans les deux cas $a^2 + b^2 = 1$.

Le fait, pour *f*, d'être représentée dans une base orthonormée par une matrice de type (I) est une propriété de *f indépendante* de la base orthonormée choisie. Nous avons appelé **rotation vectorielle de** $\mathcal{E}_2$ toute isométrie représentée dans une base orthonormée par une matrice du type (I).

Désignant par $\mathcal{R}$ l'ensemble des rotations vectorielles de $\mathcal{E}_2$ et par $\mathbf{O}_2^+$ l'ensemble des matrices du type (I), nous avons vu que la bijection

$$\begin{array}{ccc} \mathcal{R} & \longrightarrow & \mathbf{O}_2^+ \\ f & \longmapsto & \mathbf{M}(f) \end{array}$$

définit un *isomorphisme* des groupes $(\mathcal{R}, \circ)$ et $(\mathbf{O}_2^+, \times)$; rappelons que l'on note aussi $\mathbb{U}$ l'ensemble $\mathbf{O}_2^+$.

c) Angles de $\mathcal{E}_2$. Groupe $(\mathcal{A}, +)$.

On appelle **demi-droite vectorielle** de vecteur directeur $\vec{v}$ $(\vec{v} \neq \vec{0})$ l'ensemble D des vecteurs $\lambda\vec{v}$ où $\lambda \in \mathbb{R}_+$.

Étant données deux demi-droites quelconques D et D′ de $\mathcal{E}_2$, il existe une rotation unique *f* de $\mathcal{E}_2$ telle que $f(\mathrm{D}) = \mathrm{D}'$. En utilisant une relation d'équivalence ceci nous a conduit à la notion d'**angle** des demi-droites D et D′.

Désignant par $\mathcal{A}$ l'ensemble des angles de $\mathcal{E}_2$ l'application

$$\begin{array}{ccc} \mathcal{R} & \longrightarrow & \mathcal{A} \\ f & \longmapsto & \varphi \end{array}$$

qui à *f*, telle que $f(\mathrm{D}) = \mathrm{D}'$, associe l'angle $\varphi = \text{angle}(\mathrm{D}, \mathrm{D}')$, est une *bijection*. On munit alors $\mathcal{A}$ d'une addition telle que cette bijection définisse un *isomorphisme* de $(\mathcal{R}, \circ)$ sur $(\mathcal{A}, +)$.

Étant donnés deux vecteurs $\vec{v}$ et $\vec{v'}$ **non nuls** de $\mathcal{E}_2$ l'**angle des deux vecteurs** $\vec{v}$ et $\vec{v'}$ noté angle $(\vec{v}, \vec{v'})$ est par définition l'angle des demi-droites vectorielles définies respectivement par $\vec{v}$ et $\vec{v'}$.

d) Orientation du plan vectoriel $\mathcal{E}_2$.

Nous avons vu, en Première que par rapport à une base orthonormée quelconque toute rotation f de $\mathcal{E}_2$ a une matrice du type (I). D'une manière plus précise cette matrice $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$, avec $a^2 + b^2 = 1$, est telle que a et $|b|$ ne dépendent que de f et pas de la base orthonormée choisie. Il en résulte une partition des bases orthonormées de $\mathcal{E}_2$ en deux classes

L'ensemble des bases orthonormées où $M(f) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

L'ensemble des bases orthonormées où $M(f) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Deux bases sont de même sens si elles appartiennent à la même classe, de sens contraire si elles appartiennent respectivement à deux classes distinctes.

Orienter le plan euclidien $\mathcal{E}_2$ c'est

1. Choisir une base orthonormée $(\vec{u}, \vec{v})$ de $\mathcal{E}_2$.
2. Faire une partition des bases orthonormées de $\mathcal{E}_2$ en deux classes :

- La classe des bases orthonormées de **sens positif :** celles ayant le même sens que $(\vec{u}, \vec{v})$.
- La classe des bases orthonormées de **sens négatif :** celles qui sont de sens contraire avec $(\vec{u}, \vec{v})$.

Par conséquent si f est une rotation de $\mathcal{E}_2$ *orienté*, par rapport à *toute base orthonormée de sens positif* on aura

$$M(f, \vec{u}, \vec{v}) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad \text{avec} \quad a^2 + b^2 = 1;$$

on pose alors

$$a = \operatorname{Cos} f$$
$$b = \operatorname{Sin} f$$

On définit ainsi deux applications Cos et Sin de $\mathcal{R}$ dans $\mathbb{R}$.
Si φ est l'angle associé à la rotation f on dira également que a est le Cosinus de φ et b le Sinus de φ.
Notons bien que Cos et Sin s'écrivent ici avec un C et un S majuscules.

4. 12 HOMOMORPHISME θ DE $(\mathbb{R}, +)$ SUR $(\mathcal{A}, +)$. ARGUMENT D'UN NOMBRE COMPLEXE

a) Homomorphisme θ.

Nous avons vu en Première qu'il existe une application θ de $\mathbb{R}$ *sur* $\mathcal{A}$ telle que pour tout x et tout x' de $\mathbb{R}$ on ait

$$\theta(x + x') = \theta(x) + \theta(x').$$

L'application θ est un *homomorphisme surjectif* de $(\mathbb{R}, +)$ sur $(\mathcal{A}, +)$.
Le nombre π et le plus petit nombre réel strictement positif tel que $\theta(\pi)$ soit égal à l'angle plat, c'est-à-dire l'angle $(\vec{v}, -\vec{v})$ $(\vec{v} \neq \vec{0})$.

Les fonctions cosinus et sinus **fonctions réelles de variable réelle** sont alors définies pour tout x de $\mathbb{R}$ par

$$\cos x = \mathrm{Cos}\ \theta\ (x),$$
$$\sin x = \mathrm{Sin}\ \theta\ (x);$$

on remarquera que ces fonctions *numériques* de *variable réelle* sont notées avec c et s minuscules.
On a montré ensuite que $\mathbb{R}/2\pi\mathbb{Z}$ ensemble des **nombres réels** modulo 2π peut être muni d'une addition telle que $(\mathbb{R}/2\pi\mathbb{Z}, +)$ soit un groupe isomorphe à $(\mathcal{A}, +)$. Si on écrit

$$\begin{array}{ccc} \mathbb{R}/2\pi\mathbb{Z} & \longrightarrow & \mathcal{A}. \\ \dot{x} & \longmapsto & \varphi \end{array}$$

le nombre réel modulo 2π noté $\dot{x}$ est appelé **mesure** de l'angle φ; tout réprésentant $x \in \mathbb{R}$ de $\dot{x}$ est appelé **détermination** de l'angle φ.
Tout ceci peut se résumer dans le schéma

$$\begin{array}{ccccccc} & & & & (\mathbb{R}, +) & & \\ & & & & \downarrow \theta & & \\ (\mathbf{O}_2^+, \times) & \longrightarrow & (\mathcal{R}, \circ) & \longrightarrow & (\mathcal{A}, +) & \longrightarrow & (\mathbb{R}/2\pi\mathbb{Z}, +) \\ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} & \longmapsto & f & \longmapsto & \varphi & \longmapsto & \dot{x} \end{array}$$

(avec $a^2 + b^2 = 1$) et où toutes les applications marquées **sauf** θ définissent des **isomorphismes de groupes commutatifs.**
Remarquons que $\mathbf{O}_2^+$ se note aussi $\mathbb{U}$ ensemble des nombres complexes de module 1.
De plus si x est un représentant de $\dot{x}$ on a

$$\cos x = \mathrm{Cos}\, f = \mathrm{Cos}\ \varphi = a,$$
$$\sin x = \mathrm{Sin}\, f = \mathrm{Sin}\ \varphi = b,$$

avec

$$f(\vec{u}) = a\vec{u} + b\vec{v},$$
$$f(\vec{v}) = -b\vec{u} + a\vec{v},$$

où $(\vec{u}, \vec{v})$ est une base orthonormée de sens positif de $\mathcal{E}_2$.

b) Argument d'un nombre complexe de module 1.

Soit $z_0 = a + bi$ avec $a^2 + b^2 = 1$; désignons par M_0 l'image de z_0 dans le plan euclidien E_2 rapporté à $(O, \vec{u}, \vec{v})$, la base orthonormée $(\vec{u}, \vec{v})$ de $\mathcal{E}_2$ étant de sens positif (fig. 5).
Posons

$$\varphi = \text{angle}\ (\overrightarrow{OU}, \overrightarrow{OM_0})$$

et désignons enfin par α une détermination de φ; nous dirons que φ est **l'Argument de** z_0 et α **un argument** de z_0; nous écrivons

$$\varphi = \mathrm{Arg}\ z_0,$$
$$\alpha = \arg z_0;$$

si α' est une autre détermination de φ nous aurons

$$\alpha' \equiv \alpha \qquad (\text{modulo } 2\pi).$$

Le nombre complexe $a + bi$ ($a^2 + b^2 = 1$) n'est autre que $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ on a donc

$$a = \text{Cos } \varphi = \cos \alpha,$$
$$b = \text{Sin } \varphi = \sin \alpha.$$

Le nombre complexe z_0 de module 1 s'écrit donc

$$z_0 = \cos \alpha + i \sin \alpha$$

où $\alpha \in \mathbb{R}$. De plus quels que soient α et α' de $\mathbb{R}$

$$\boxed{(\cos \alpha + i \sin \alpha = \cos \alpha' + i \sin \alpha') \iff (\alpha \equiv \alpha' \text{ (modulo } 2\pi))}$$

REMARQUE

1. On notera l'usage des majuscules et des minuscules dans les écritures suivantes :

$$z_0 = a + bi \qquad a^2 + b^2 = 1$$
$$a = \text{Cos (Arg } z_0) = \cos (\arg z_0)$$
$$b = \text{Sin (Arg } z_0) = \sin (\arg z_0).$$

c) Argument d'un nombre complexe non nul.

Nous avons vu au § 4.9 d que tout nombre complexe $z = a + bi$ **non nul** peut s'écrire d'une manière unique sous la forme

$$z = |z| z_0 \quad \text{avec} \quad |z_0| = 1;$$

nous poserons par définition

$$\text{Arg } z = \text{Arg } z_0,$$
$$\arg z = \arg z_0.$$

Donc si r est le module de z et α un argument de z, on a

$$z = r (\cos \alpha + i \sin \alpha)$$

dans le cas étudié $r > 0$.
Quels que soient les réels α, α' et $r > 0$, $r' > 0$, on a :

$$r (\cos \alpha + i \sin \alpha) = r' (\cos \alpha' + i \sin \alpha') \iff \begin{cases} r = r' \\ \alpha \equiv \alpha' \pmod{2\pi} \end{cases}$$

Quel que soit $\alpha \in \mathbb{R}$ on a

$$0 \times (\cos \alpha + i \sin \alpha) = 0$$

nous dirons que, quels que soient $r \in \mathbb{R}_+$ et $\alpha \in \mathbb{R}$,

$$\boxed{z = r (\cos \alpha + i \sin \alpha)}$$

est **une forme trigonométrique** du nombre z; si $r > 0$, α est « déterminé à $2k\pi$ près, ($k \in \mathbb{Z}$) »; si $r = 0$, α est un nombre réel quelconque.

EXEMPLES

1. Soit $z = 1 + i$ on a $r^2 = 2$ d'où $r = \sqrt{2}$

$$z = \sqrt{2} \left(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}} \right) = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right)$$

$$\text{donc} \quad r = \sqrt{2}$$
$$\arg z \equiv \frac{\pi}{4} \pmod{2\pi}$$

2. Soit $z = a \in \mathbb{R}$
Si $a > 0$ $r = a$ $\arg z \equiv 0 \pmod{2\pi}$
$$a = a(\cos 0 + i \sin 0).$$
Si $a < 0$ $r = -a$ $\arg z \equiv \pi \pmod{2\pi}$
$$a = (-a)(\cos \pi + i \sin \pi).$$
3. Soit $z = (-5)(\cos \alpha + i \sin \alpha)$ on a
$$z = 5[\cos(\alpha + \pi) + i \sin(\alpha + \pi)]$$
c'est-à-dire $r = 5$ et
$$\arg z \equiv \alpha + \pi \pmod{2\pi}.$$

D'une manière générale si
$$z = a(\cos \alpha + i \sin \alpha), \qquad a \in \mathbb{R}^*, \alpha \in \mathbb{R}$$
α est un argument de z si et seulement si $a > 0$. Si $a < 0$ on a
$$z = (-a)(\cos(\alpha + \pi) + i \sin(\alpha + \pi))$$
et par conséquent $|z| = -a$ et $\arg z \equiv \alpha + \pi \pmod{2\pi}$.

EXERCICE

1. Trouver le module et l'argument des nombres complexes suivants :
$$\frac{1 - i\sqrt{3}}{2}, \quad 3i, \quad -\frac{5}{2}i.$$

d) Relations entre forme algébrique et forme trigonométrique d'un nombre complexe.

Soit un nombre complexe *non nul*
$$z = x + iy = r(\cos \alpha + i \sin \alpha)$$
où x, y, α sont des nombres réels et r un nombre réel **strictement positif**. On a
$$\boxed{\begin{aligned} x &= r \cos \alpha \\ y &= r \sin \alpha \end{aligned}}$$

On en déduit puisque $r > 0$ et $r^2 = x^2 + y^2$
$$\boxed{\begin{aligned} r &= \sqrt{x^2 + y^2} \\ \cos \alpha &= \frac{x}{\sqrt{x^2 + y^2}} \\ \sin \alpha &= \frac{y}{\sqrt{x^2 + y^2}} \end{aligned}}$$

Les formules $\cos \alpha = \frac{x}{r}$ et $\sin \alpha = \frac{y}{r}$ permettent de déterminer un réel modulo 2π; on calculera un représentant α de la classe $\dot{x}$, modulo 2π.
Si $x \neq 0$ on a aussi
$$\operatorname{tg} \alpha = \frac{y}{x};$$
mais cette formule, souvent utile, ne détermine pas α; elle détermine seulement α « à $k\pi$ près » ($k \in \mathbb{Z}$).

REMARQUE

2. Dans tout ce qui précède (§ 4.11 et 4.12), pour soulager la mémoire, les lettres θ, φ, α... ont été utlisées pour représenter des objets bien précis : θ homomorphisme de $(\mathbb{R}, +)$ sur $(\mathcal{A}, +)$, φ angle de deux vecteurs, $\alpha \in \mathbb{R}$ détermination d'un angle ou argument d'un nombre complexe.
Désormais nous « libérons ces lettres » c'est-à-dire que θ, φ, α pourront représenter d'autres objets que ceux décrits plus haut. En particulier on désigne souvent un argument d'un nombre complexe par θ ou φ, θ ou φ représentent alors des nombres réels.

EXERCICE

2. La lettre φ désignant un nombre réel quelconque trouver module et argument des nombres complexes

$$z_1 = 1 + \cos\varphi + i\sin\varphi,$$
$$z_2 = \sin\varphi + i(1 + \cos\varphi),$$
$$z_3 = \cos\varphi + i(1 + \sin\varphi).$$

On discutera dans chaque cas suivant les valeurs de φ.

4. 13 PRODUIT ET QUOTIENT DE NOMBRES COMPLEXES DONNÉS SOUS FORME TRIGONOMÉTRIQUE

a) Produit de deux ou plusieurs nombres complexes.

Soit deux nombres complexes non nuls ($r > 0$, $r' > 0$, $\alpha \in \mathbb{R}$, $\alpha' \in \mathbb{R}$)

$$z = r(\cos\alpha + i\sin\alpha)$$
$$z' = r'(\cos\alpha' + i\sin\alpha').$$

On en déduit :

$$zz' = rr'[\cos\alpha\cos\alpha' - \sin\alpha\sin\alpha' + i(\cos\alpha\sin\alpha' + \sin\alpha\cos\alpha')]$$
$$= rr'[\cos(\alpha + \alpha') + i\sin(\alpha + \alpha')].$$

Nous avons donc :

$$\boxed{\begin{array}{l} |zz'| = |z|\,|z'| \\ \arg(zz') \equiv \arg(z) + \arg(z') \qquad [2\pi] \end{array}}$$

REMARQUE

1. Pour des nombres complexes de module 1, la seconde relation traduit l'isomorphisme de $(\mathbf{O}_2^+, \times)$ sur $(\mathbb{R}/2\pi\mathbb{Z}, +)$.

EXERCICES

1. Soit n nombres complexes :

$$z_k = r_k(\cos\alpha_k + i\sin\alpha_k) \qquad (k = 1, 2\ldots, n).$$

Calculer le module et l'argument du produit de ces n nombres (on fera un raisonnement par récurrence).

2. On donne le nombre complexe ($k > 0$, $\varphi \in \mathbb{R}$)

$$a = k(\cos\varphi + i\sin\varphi).$$

A tout point M d'affixe $z = x + iy = r(\cos\theta + i\sin\theta)$ on associe le point M' d'affixe $z' = x' + iy' = r'(\cos\theta' + i\sin\theta')$ tel que

(1) $$z' = az.$$

a) Calculer x', y', en fonction de x, y, k, φ.

b) Démontrer que

$$\begin{cases} \| \overrightarrow{OM'} \| = k \| \overrightarrow{OM} \| \\ (\widehat{\overrightarrow{OM}, \overrightarrow{OM'}}) = \dot{\varphi} \end{cases}$$

Quelle est l'application $M \longmapsto M'$ lorsque a est *réel?*
Si $k = 1$ l'application $M \longmapsto M'$ est appelée **rotation** de E_2 de centre O et d'angle φ (c'est-à-dire dont l'angle a pour détermination φ); on la note $R(O, \varphi)$.

c) Revenant au cas général et notant $H(O, k)$ l'homothétie de centre O et de rapport k, démontrer que l'application $M \longmapsto M'$ est égale à

$$H(O, k) \circ R(O, \varphi) = R(O, \varphi) \circ H(O, k).$$

Cette bijection de E_2 dans E_2 est appelée **similitude** de centre O, de rapport k et d'angle φ, on la note $S(O, k, \varphi)$.

d) Par analogie avec (1) si $\overrightarrow{OM} = \vec{v}$ et $\overrightarrow{OM'} = \vec{v'}$ on posera

(2) $$\vec{v'} = a\vec{v}.$$

Démontrer que $\vec{v} \longmapsto \vec{v'}$ est une bijection s de $\mathcal{E}_2$; décomposer s à l'aide d'une homothétie et d'une rotation vectorielles.

3. On rapporte $\mathcal{E}_2$ à deux bases *orthonormées* de *même sens* $(\vec{u}, \vec{v})$ et $(\vec{U}, \vec{V})$ telles que

$$\vec{U} = (\cos \alpha + i \sin \alpha)\, \vec{u}.$$

a) Démontrer que $\vec{v} = i\vec{u}$ et $\vec{V} = i\vec{U}$.

b) Soit M un point de E_2, ses coordonnées sont (x, y) dans le repère $(O, \vec{u}, \vec{v})$ et (X, Y) dans le repère $(O, \vec{U}, \vec{V})$. Calculer x, y en fonction de X, Y, α; on montrera d'abord que $x + iy = (\cos \alpha + i \sin \alpha)(X + iY)$.

b) Puissance entière positive d'un nombre complexe.

Supposons que les n nombres complexes donnés soient égaux à $(\cos \alpha + i \sin \alpha)$, on a

$$\boxed{(\cos \alpha + i \sin \alpha)^n = \cos n\alpha + i \sin n\alpha}.$$

Remarquons que cette formule est valable pour $n = 0$ et en convenant que $z^0 = 1$ (pour $z \neq 0$). Elle est très utile pour calculer $\cos n\alpha$ et $\sin n\alpha$.

EXEMPLES

1. Si l'on veut calculer $\cos 3\alpha$ et $\sin 3\alpha$ en fonction de $\cos \alpha$ et $\sin \alpha$, nous calculerons : $(\cos \alpha + i \sin \alpha)^3$. On a

$$\begin{aligned} (\cos \alpha + i \sin \alpha)^3 &= \cos^3 \alpha + 3i \cos^2 \alpha \sin \alpha - 3 \cos \alpha \sin^2 \alpha - i \sin^3 \alpha \\ &= \cos 3\alpha + i \sin 3\alpha. \end{aligned}$$

Nous avons ainsi écrit un nombre complexe de deux façons différentes, sous forme algébrique : les parties réelles et imaginaires sont égales, d'où :

$$\begin{cases} \cos 3\alpha = \cos^3 \alpha - 3 \cos \alpha \sin^2 \alpha, \\ \sin 3\alpha = 3 \cos^2 \alpha \sin \alpha - \sin^3 \alpha. \end{cases}$$

Si $\cos 3\alpha \neq 0$ on en déduit

$$\operatorname{tg} 3\alpha = \frac{3 \operatorname{tg} \alpha - \operatorname{tg}^3 \alpha}{1 - 3 \operatorname{tg}^2 \alpha}.$$

On en déduit en utilisant la formule $\cos^2 \alpha + \sin^2 \alpha = 1$,

$$\begin{cases} \cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha, \\ \sin 3\alpha = 3 \sin \alpha - 4 \sin^3 \alpha. \end{cases}$$

2. On a de même

$$(\cos\alpha + i\sin\alpha)^4 = \cos^4\alpha + 4i\cos^3\alpha\sin\alpha - 6\cos^2\alpha\sin^2\alpha - 4i\cos\alpha\sin^3\alpha + \sin^4\alpha$$

car $i^3 = -i$ et $i^4 = 1$; on a donc

$$\begin{cases} \cos 4\alpha = \cos^4\alpha - 6\cos^2\alpha\sin^2\alpha + \sin^4\alpha \\ \sin 4\alpha = 4(\cos^3\alpha\sin\alpha - \cos\alpha\sin^3\alpha) \end{cases}$$

On voit que $\cos 4\alpha$ peut s'exprimer par un polynôme en $\cos\alpha$ ou un polynôme en $\sin\alpha$.

Dans un exercice de la fin du chapitre nous verrons que P, Q, R désignant des polynomes à coefficients réels on a

$\cos n\alpha = P(\cos\alpha)$ pour tout entier naturel n

$\cos n\alpha = Q(\sin\alpha)$ pour tout entier naturel **pair** n

$\sin n\alpha = R(\sin\alpha)$ pour tout entier naturel **impair** n.

c) Quotient de deux nombres complexes.

Inverse d'un nombre complexe non nul.

Soit $z = r(\cos\alpha + i\sin\alpha)$, un nombre complexe non nul ($r > 0$).
Son inverse est un nombre z' tel que $zz' = 1$.
D'après ce qui précède :

$$|zz'| = |z||z'| = 1.$$
$$\arg(zz') \equiv \arg(z) + \arg(z') \equiv 0 \quad [2\pi].$$

Par suite :

$$\begin{cases} |z'| = \dfrac{1}{|z|} \\ \arg(z') \equiv -\arg(z) \quad [2\pi]. \end{cases}$$

En particulier, si $z = \cos\alpha + i\sin\alpha$, $z' = \cos\alpha - i\sin\alpha = \bar{z}$.

Quotient de deux nombres complexes.

Soit z_1 et z_2 deux nombres complexes tels que :

$$z_1 = r_1(\cos\alpha_i + i\sin\alpha_1),$$
$$z_2 = r_2(\cos\alpha_2 + i\sin\alpha_2) \neq 0.$$

Le quotient $\dfrac{z_1}{z_2}$ est égal à $z_1 \times \dfrac{1}{z_2}$. D'où :

$$\left|\frac{z_1}{z_2}\right| = |z_1| \times \left|\frac{1}{z_2}\right| = |z_1| \times \frac{1}{|z_2|}, \quad \text{et :}$$

$$\arg\left(\frac{z_1}{z_2}\right) \equiv \arg(z_1) + \arg\left(\frac{1}{z_2}\right) \equiv \arg(z_1) - \arg(z_2) \quad [2\pi]$$

$$\boxed{\begin{aligned} \left|\frac{z_1}{z_2}\right| &= \frac{|z_1|}{|z_2|} \\ \arg\left(\frac{z_1}{z_2}\right) &\equiv \arg(z_1) - \arg(z_2) \quad [2\pi] \end{aligned}}$$

d) Formule de Moivre.

Nous avons démontré que, pour tout n entier naturel on a

(1) $$(\cos \alpha + i \sin \alpha)^n = \cos n\,\alpha + i \sin n\,\alpha;$$

et aussi que, si $z = \cos \alpha + i \sin \alpha$, alors :

(2) $$\frac{1}{z} = \cos \alpha - i \sin \alpha.$$

Nous nous proposons de calculer $(\cos \alpha + i \sin \alpha)^n$ pour tout entier relatif n.
Si n est un entier positif, la formule (1) nous donne le résultat.
Si n est un entier négatif

$$\begin{aligned}(\cos \alpha + i \sin \alpha)^n &= \frac{1}{(\cos \alpha + i \sin \alpha)^{-n}} \qquad (\text{avec } -n \in \mathbb{N}) \\ &= \frac{1}{\cos(-n\,\alpha) + i \sin(-n\,\alpha)} \text{ (d'après (1)} \\ &= \cos(-n\,\alpha) - i \sin(-n\,\alpha) \text{ (d'après (2)} \\ &= \cos n\,\alpha + i \sin n\,\alpha.\end{aligned}$$

Il est donc établi que

> Quel que soit $n \in \mathbb{Z}$:
> $(\cos \alpha + i \sin \alpha)^n = \cos n\,\alpha + i \sin n\,\alpha$

Cette formule s'appelle formule de MOIVRE.

4. 14 RACINES $n^{\text{ièmes}}$ D'UN NOMBRE COMPLEXE

a) Racines $n^{\text{ièmes}}$ d'un nombre complexe.

Nous nous proposons de déterminer tous les nombres complexes z tels que $z^n = Z$ où Z est un nombre complexe donné non nul et n un entier naturel donné non nul. Un tel nombre z, s'il existe, sera appelé racine $n^{\text{ième}}$ de Z. Le nombre donné Z a pour module r et pour argument α. Appelons ρ et θ le module et l'argument du nombre z cherché. D'après ce qui précède

$$z^n = \rho^n (\cos n\,\theta + i \sin n\,\theta).$$

Or $$Z = r(\cos \alpha + i \sin \alpha).$$

L'égalité $z^n = Z$ est donc possible si et seulement si :

$$\begin{cases} \rho^n = r, \\ \text{et} \quad n\,\theta = \alpha + k\,2\pi \qquad (k \in \mathbb{Z}) \end{cases}$$

Si $r > 0$, nous avons vu au § 2.13 qu'il existe un nombre réel $\rho > 0$ unique tel que $\rho^n = r$, c'est $\sqrt[n]{r}$; on a donc $z^n = Z$ si seulement si :

$$\begin{cases} \rho = \sqrt[n]{r} \\ \text{et} \quad \theta = \dfrac{\alpha}{n} + k\,\dfrac{2\pi}{n} \qquad (k \in \mathbb{Z}). \end{cases}$$

Le module de z est déterminé de façon unique. Son argument a n valeurs possibles distinctes dans $\mathbb{R}/2\pi\mathbb{Z}$; elles correspondent à *n valeurs consécutives de l'entier k.*

Il existe donc n racines $n^{\text{ièmes}}$ distinctes de Z. On peut les écrire :

$$z_k = \sqrt[n]{r}\left(\cos\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right) + i\sin\left(\frac{\alpha}{n} + k\frac{2\pi}{n}\right)\right)$$
avec $k \in \{0, 1, \ldots, n-1\}$.

Théorème.

Tout nombre complexe non nul a n racines n^{iemes} distinctes ; ces n racines ont même module et des arguments différant de $k\frac{2\pi}{n}$ où $k = 0, 1, \ldots, n-1$.

On voit que dans le plan euclidien ces n racines sont situées sur un cercle de centre O et de rayon $\rho = \sqrt[n]{r}$; ces images sont les sommets d'un polygone régulier de n côtés tout au moins si $n \geqslant 3$.

EXEMPLES

1. Si $n = 2$ on trouve, pour $Z = r(\cos\alpha + i\sin\alpha)$ où $r > 0$,

$$z_0 = \sqrt{r}\left(\cos\frac{\alpha}{2} + i\sin\frac{\alpha}{2}\right),$$

$$z_1 = \sqrt{r}\left(\cos\left(\frac{\alpha}{2} + \pi\right) + i\sin\left(\frac{\alpha}{2} + \pi\right)\right) = -z_0.$$

On retrouve donc sous forme trigonométrique les deux racines carrées opposées obtenues sous forme algébrique au § 4.10 a.

2. Résolvons l'équation $z^3 = 1$.
Avec les mêmes notations que précédemment, nous obtenons :

$$\begin{cases} \rho = 1. \\ \text{et} \\ \theta = k\frac{2\pi}{3} \qquad (\text{puisque } \alpha = 0) \end{cases}$$

avec $k = 0, 1, 2$.

D'où :

$$z_0 = 1$$

$$z_1 = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right) = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$

$$z_2 = \cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right) = -\frac{1}{2} - i\frac{\sqrt{3}}{2}.$$

Les mathématiciens ont l'habitude de poser

$$j = -\frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

On a donc

$$z_1 = j$$
$$z_2 = j^2 = \bar{j}$$

Les racines cubiques de 1 sont donc $1, j, j^2 = \bar{j}$. Comme $|j| = 1$ on a aussi $j^2 = \bar{j} = \frac{1}{j}$; on vérifiera également que $1 + j + j^2 = 0$.

EXERCICE

1. Calculer sous forme algébrique et sous forme trigonométrique les racines carrées et les racines cubiques de i et $-i$.

Remarque sur les notations.

Les physiciens et en particulier les électriciens, désignant l'intensité de courant par la lettre i, désignent par j le nombre complexe noté i par les mathématiciens; les physiciens notent le nombre $-\frac{1}{2} + i\frac{\sqrt{3}}{2}$ par une lettre distincte de j, ω en général; dans les ouvrages d'électricité on a donc $j^2 = -1$ et $\omega^3 = 1$.

b) Racines $n^{\text{ièmes}}$ de l'unité.

Si $Z = 1, r = 1$ et $\alpha = 0$.

Donc $\rho = 1$ et $\theta = k\frac{2\pi}{n}$ avec $k \in \{0, 1, \ldots, n-1\}$.

Les n racines $n^{\text{ièmes}}$ de l'unité sont donc les nombres complexes

$$\cos k\frac{2\pi}{n} + i \sin k\frac{2\pi}{n}$$

avec $k \in \{0, 1, \ldots, n-1\}$.

EXERCICE

2. Notant $\mathbb{U}_n$ l'ensemble des racines $n^{\text{ièmes}}$ de 1, démontrer que $(\mathbb{U}_n, \times)$ est un sous-groupe de $(\mathbb{U}, \times)$ et de $(\mathbb{C}^*, \times)$.
Étudier les images des éléments de $\mathbb{U}_n$ dans le plan euclidien. On fera les figures dans les cas $n = 3, 4, 5, 6, 8$.
Calculer ces racines sous forme algébrique pour $n = 4, 6, 8$.

Soit z une racine $n^{\text{ième}}$ quelconque de $Z \neq 0$, choisissons-en une a, on a donc

$$Z = z^n = a^n$$

ou encore

$$\left(\frac{z}{a}\right)^n = 1.$$

On en déduit

$$\frac{z}{a} = \cos k\frac{2\pi}{n} + i \sin k\frac{2\pi}{n} \qquad (k = 0, 1 \ldots, n-1)$$

On obtient les n racines n^{iemes} d'un nombre complexe en multipliant l'une d'entre elle par les n racines n^{iemes} de l'unité.

Soit par exemple $Z = -8$, (-2) est une des racines cubiques de -8, donc l'ensemble des racines cubiques de -8 est $\{-2, -2j, -2\bar{j}\}$.

EXERCICE

3. Les racines $n^{\text{ièmes}}$ d'un nombre complexe Z non nul forment-elles un groupe multiplicatif?
Étudier la disposition des images des racines $n^{\text{ièmes}}$ d'un nombre complexe Z non nul dans le plan euclidien E_2 dans les cas suivants :

$$Z_1 = -1 + i, \qquad n_1 = 3;$$
$$Z_2 = 4(\sqrt{3} - i), \qquad n_2 = 6;$$
$$Z_3 = -9i \qquad n_3 = 4.$$

4. 15 FORMULES DE TRIGONOMÉTRIE (RÉVISION ET COMPLÉMENTS)

Les formules

$$\cos(a+b) = \cos a \cos b - \sin a \sin b,$$
$$\sin(a+b) = \sin a \cos b + \cos a \sin b,$$

nous ont permis de trouver l'argument d'un produit. Inversement le calcul de $(\cos a + i + \sin a)(\cos b + i \sin b)$ permet de *retrouver* ces formules (ce calcul ne constitue évidemment pas une démonstration).

Pour la commodité du lecteur nous regroupons ici toutes les conséquences de ces formules : certaines des relations que l'on obtient ainsi ont déjà été données en Première, d'autres sont nouvelles; elles seront toutes utilisées dans la suite, en particulier dans le tome 2.

a) Révision des formules obtenues en Première.

Quels que soient les nombres réels a et b on a

$$\boxed{\begin{aligned}\cos(a+b) &= \cos a \cos b - \sin a \sin b \quad (1)\\ \cos(a-b) &= \cos a \cos b + \sin a \sin b \quad (2)\\ \sin(a+b) &= \sin a \cos b + \cos a \sin b \quad (3)\\ \sin(a-b) &= \sin a \cos b - \cos a \sin b \quad (4)\end{aligned}}$$

Quels que soient $a \neq \frac{\pi}{2} + k\pi$, $b \neq \frac{\pi}{2} + k\pi$ et pourvu que $a + b \neq \frac{\pi}{2} + k\pi$, $(k \in \mathbb{Z})$

$$\boxed{\operatorname{tg}(a+b) = \frac{\operatorname{tg} a + \operatorname{tg} b}{1 - \operatorname{tg} a \operatorname{tg} b}} \quad (5)$$

Quels que soient $a \neq \frac{\pi}{2} + k\pi$, $b \neq \frac{\pi}{2} + k\pi$ et pourvu que $a - b \neq \frac{\pi}{2} + k\pi$, $(k \in \mathbb{Z})$

$$\boxed{\operatorname{tg}(a-b) = \frac{\operatorname{tg} a - \operatorname{tg} b}{1 + \operatorname{tg} a \operatorname{tg} b}} \quad (6)$$

EXERCICES

1. Calculer le cosinus, le sinus et la tangente des nombres suivants :

$$\frac{7\pi}{12} \quad , \quad \frac{5\pi}{12} \quad , \quad \frac{11\pi}{12} \quad , \quad \frac{\pi}{12}.$$

2. Simplifier les expressions suivantes, quand elles sont définies :

$$\frac{1 + \operatorname{tg} a}{1 - \operatorname{tg} a} \quad , \quad \frac{1 - \operatorname{tg} a}{1 + \operatorname{tg} a}.$$

De ces formules, nous avons déduit les résultats suivants :

Quel que soit le nombre réel a, on a

$$\boxed{\begin{aligned}\cos 2a &= \cos^2 a - \sin^2 a = 2\cos^2 a - 1 = 1 - 2\sin^2 a \quad (7)\\ \sin 2a &= 2 \sin a \cos a. \quad (8)\end{aligned}}$$

Quel que soit le nombre réel $a \neq \frac{\pi}{4} + k\frac{\pi}{2}$ et $a \neq \frac{\pi}{2} + k\,\pi$, on a

$$\boxed{\operatorname{tg} 2a = \frac{2 \operatorname{tg} a}{1 - \operatorname{tg}^2 a}} \tag{9}$$

De (7), on déduit des formules valables pour tout a réel

$$\boxed{\cos^2 a = \frac{1 + \cos 2a}{2}} \tag{10}$$

$$\boxed{\sin^2 a = \frac{1 - \cos 2a}{2}} \tag{11}$$

D'autre part, pour tout $x \neq \pi + k\,2\pi$, et en posant $\operatorname{tg}\frac{x}{2} = t$, il en a résulté

$$\boxed{\cos x = \frac{1 - t^2}{1 + t^2}} \tag{12}$$

$$\boxed{\sin x = \frac{2t}{1 + t^2}} \tag{13}$$

$$\boxed{\operatorname{tg} x = \frac{2t}{1 - t^2}} \tag{14}$$

(pour la formule (14), on suppose $x \neq \pi + k\,2\pi$ et $x \neq \frac{\pi}{2} + k\,\pi$).

b) Formules de transformation de produits en sommes.

Des formules (1) et (2), il résulte que pour tout a et b réels :

$$\boxed{\cos a \cos b = \frac{1}{2}[\cos(a + b) + \cos(a - b)]} \tag{15}$$

$$\boxed{\sin a \sin b = \frac{1}{2}[\cos(a - b) - \cos(a + b)]} \tag{16}$$

et de (3) et (4),

$$\boxed{\sin a \cos b = \frac{1}{2}[\sin(a + b) + \sin(a - b)]} \tag{17}$$

$$\boxed{\cos a \sin b = \frac{1}{2}[\sin(a + b) - \sin(a - b)]} \tag{18}$$

EXEMPLE

1. Pour tout x réel on a

$$16 \cos^3 x \sin^2 x = 4 \cos x (2 \sin x \cos x)^2 = 4 \cos x \sin^2 2x$$
$$= 2 \cos x (1 - \cos 4x) = 2 \cos x - (\cos 3x + \cos 5x)$$
$$= 2 \cos x - \cos 3x - \cos 5x.$$

c) Formules de transformation de sommes en produits.

Dans la formule (15), posons $a + b = p$ et $a - b = q$.

Nous en déduisons, $a = \frac{p+q}{2}$ et $b = \frac{p-q}{2}$; d'où :

$$\cos p + \cos q = 2 \cos \frac{p+q}{2} \cos \frac{p-q}{2} \tag{19}$$

De même, en utilisant les formules (16), (17) et (18), quels que soient p et q réels

$$\cos p - \cos q = -2 \sin \frac{p+q}{2} \sin \frac{p-q}{2} \tag{20}$$

$$\sin p + \sin q = 2 \sin \frac{p+q}{2} \cos \frac{p-q}{2} \tag{21}$$

$$\sin p - \sin q = 2 \cos \frac{p+q}{2} \sin \frac{p-q}{2} \tag{22}$$

EXEMPLE

2. Pour tout x réel on a

$$\begin{aligned} 2 \cos x - \cos 3x - \cos 5x &= 2 \cos x - 2 \cos 4x \cos x \\ &= 2 \cos x (1 - \cos 4x) = 4 \cos x \sin^2 2x = 4 \cos x (2 \sin x \cos x)^2 \\ &= 16 \cos^3 x \sin^2 x. \end{aligned}$$

EXERCICE

Transformer en produits ou quotients : $\cos p + \sin q$, $\operatorname{tg} p + \operatorname{tg} q$, $\operatorname{tg} p - \operatorname{tg} q$.

d) Factorisation et linéarisation.

Considérons la fonction F définie pour tout x réel par

$$F(x) = 16 \cos^3 x \sin^2 x = 2 \cos x - \cos 3x - \cos 5x$$

et les fonctions f_1, f_2, f_3, g_1 définies pour tout x réel par

$$f_1(x) = \cos x, \quad f_2(x) = \cos 3x, \quad f_3(x) = \cos 5x, \quad g_1(x) = \sin x$$

nous avons

$$F = 16 (f_1)^3 (g_1)^2 = 2f_1 - f_2 - f_3;$$

donc F apparaît *à la fois* comme un *produit* et comme une *combinaison linéaire* de fonctions.

Le passage de la forme $2f_1 - f_2 - f_3$ à $16 (f_1)^3 (g_1)^2$ est appelé **factorisation** de F et le passage réciproque **linéarisation** de F.

La *factorisation* sera employée lorsque $F(x)$ apparaîtra dans un calcul où l'on voudra effectuer des mises en facteur, des simplifications de quotients; naturellement la factorisation sera indispensable lorsqu'on voudra résoudre l'équation $F(x) = 0$ ou l'inéquation $F(x) \leqslant 0$.

En revanche la *linéarisation* se révélera extrêmement utile lorsqu'on voudra chercher l'image de F par une application linéaire; par exemple pour le calcul des dérivées premières, secondes, ... $n^{\text{ièmes}}$ on aura

$$\begin{aligned} F' &= 2f_1' - f_2' - f_3' \\ F^{(n)} &= 2f_1^{(n)} - f_2^{(n)} - f_3^{(n)} \end{aligned}$$

ce qui nous donne immédiatement ici

$$F^{(n)}(x) = 2\cos\left(x + n\frac{\pi}{2}\right) - 3^n\cos\left(3x + n\frac{\pi}{2}\right) - 5^n\cos\left(5x + n\frac{\pi}{2}\right).$$

Dans le cas étudié F appartient à l'ensemble des fonctions numériques dérivables un nombre quelconque de fois que nous désignerons par $\mathfrak{D}(\mathbb{R}, \mathbb{R})$; il est évident que $(\mathfrak{D}(\mathbb{R}, \mathbb{R}), +, \bullet)$ est un espace vectoriel sur $\mathbb{R}$ et que $(\mathfrak{D}(\mathbb{R}, \mathbb{R}), +, \times)$ est un anneau.

L'application « dérivation $n^{\text{ième}}$ »

$$\begin{aligned} \varphi : \mathfrak{D}(\mathbb{R}, \mathbb{R}) &\longrightarrow \mathfrak{F}(\mathbb{R}, \mathbb{R}) \\ F &\longmapsto F^{(n)} \end{aligned}$$

est une *application linéaire* de l'espace vectoriel $\mathfrak{D}(\mathbb{R}, \mathbb{R})$ dans l'espace vectoriel $\mathfrak{F}(\mathbb{R}, \mathbb{R})$ mais n'est pas un homomorphisme de l'anneau $\mathfrak{D}(\mathbb{R}, \mathbb{R})$ dans l'anneau $\mathfrak{F}(\mathbb{R}, \mathbb{R})$ car la dérivée $n^{\text{ième}}$ de FG n'est pas le produit des dérivées $n^{\text{ièmes}}$ de F et de G (le vérifier pour $n = 1$ et $n = 2$).

D'une manière générale si A est un ensemble muni d'une addition interne, d'une multiplication interne et d'une multiplication externe à opérateurs dans $\mathbb{R}$ on dit que A est une **algèbre sur** $\mathbb{R}$ si et seulement si

i. $(A, +, \times)$ est un anneau

ii. $(A, +, \bullet)$ est un espace vectoriel sur $\mathbb{R}$

iii. Quels que soient α de $\mathbb{R}$ et a et b de A on a $(\alpha a)\, b = a\,(\alpha b) = \alpha\,(ab)$.

Par exemple vous voyez sans peine que $\mathbb{C}$ est une algèbre sur $\mathbb{R}$; il en est de même de $\mathfrak{F}(\mathbb{R}, \mathbb{R})$, de $\mathfrak{D}(\mathbb{R}, \mathbb{R})$ etc.

Si on a

$$x = \alpha_1 a_1 + \ldots + \alpha_p a_p = \beta\, b_1\, b_2 \ldots b_q,$$

$x, a_1, \ldots, a_p, b_1, \ldots, b_q$ étant des éléments de A et $\alpha_1 \ldots \alpha_p$, β des réels, les deux écritures de x sous la forme linéarisée $\alpha_1 a_1 + \ldots + \alpha_p a_p$ et la forme factorisée $\beta\, b_1\, b_2 \ldots b_q$ auront des domaines d'applications différents; en particulier la linéarisation de x sera très utile sinon indispensable pour le calcul de $\varphi(x)$ lorsque

$$\varphi : A \longrightarrow A'$$

application de l'algèbre A dans l'algèbre A' *est une application linéaire* de A dans A' considérés comme *espaces vectoriels* sur $\mathbb{R}$ mais *n'est pas un homomorphisme* de A dans A' considérés comme anneau. On aura dans ce cas

$$\varphi(x) = \alpha_1 \varphi(a_1) + \ldots + \alpha_p \varphi(a_p)$$

alors que la connaissance de $\varphi(b_1) \ldots \varphi(b_q)$ ne permet pas de calculer directement $\varphi(x)$.

On voit que les deux opérations « factorisation » et « linéarisation » sont infiniment plus générales que les transformations de « sommes en produits » et de « produits en sommes », en trigonométrie, dont nous sommes partis; on en rencontrera de multiples applications en *Analyse*, en particulier pour la dérivation des fonctions numériques et pour ce que nous appellerons alors leur intégration.

EXERCICES

Espaces vectoriels (révision) : 1 à 17.
Homomorphismes de $\mathcal{U}_2$ dans $\mathcal{U}_2$ et matrices carrées d'ordre 2 (révision) : 18 à 30.
Calcul dans le corps des complexes : 31 à 40, 43, 124.
Module et argument : 41, 42 et 44 à 54.
Équations dans $\mathbb{C}$: 55 à 70.
Ensemble de points dont les affixes vérifient une relation donnée : 71 à 93.
Calculs trigonométriques : 100 à 123, 125, 126.
Suites complexes : 126, 127.
Problèmes généraux : 94 à 99.

4.1 Soit E l'ensemble des nombres réels de la forme $a + a'\sqrt{2}$, où a et a' sont des rationnels quelconques. On munit E de l'addition et de la multiplication par un rationnel quelconque suivantes :

$$(a + a'\sqrt{2}) + (b + b'\sqrt{2}) = a + b + (a' + b')\sqrt{2},$$
$$\lambda(a + a'\sqrt{2}) = \lambda a + \lambda a'\sqrt{2}.$$

Démontrer que (E, +, •) est un espace vectoriel sur $\mathbb{Q}$. Quelle est sa dimension? (Cf. exercice 3.22.)

4.2 Même question qu'à l'exercice 4.1 pour E ensemble des nombres réels de la forme

$$a\sqrt{2} + a'\sqrt{3} + a''\sqrt{5}$$

où a, a', a'' sont des rationnels quelconques. (Cf. exercice 3.23.)

4.3 On pose $\omega = \sqrt[3]{2}$. Même question qu'à l'exercice 4.1 pour E ensemble des nombres réels de la forme $a + a'\omega + a''\omega^2$ où a, a', a'' sont des rationnels quelconques. (Cf. exercice 3.24.)

On donne les vecteurs a, b, c de $E = \mathbb{R}^3$ espace vectoriel sur $\mathbb{R}$; déterminer si (a, b, c) est une base de $\mathbb{R}^3$; dans le cas contraire déterminer la dimension du sous-espace F engendré par a, b et c (ex. 4.4 à 4.7).

4.4 $a = (0, 1, 1)$, $b = (1, 0, 1)$, $c = (1, 1, 0)$.

4.5 $a = (0, 1, -1)$, $b = (-1, 0, 1)$, $c = (1, -1, 0)$.

4.6 $a = (1, 1, -2)$, $b = (-2, 1, 1)$, $c = (1, -2, 1)$.

4.7* $a = (\alpha, \beta, \gamma)$, $b = (\gamma, \alpha, \beta)$, $c = (\alpha, \beta, \gamma)$ (α, β, γ nombres réels donnés). Discuter.

4.8 On donne dans $\mathbb{R}^3$ espace vectoriel sur $\mathbb{R}$ les vecteurs

$$v_1 = (1, 0, 1) \quad v_2 = (0, 1, 0) \quad w_1 = (1, 1, 0) \quad w_2 = (0, 0, 1)$$

et on considère les sous-espaces vectoriels F engendré par v_1 et v_2 et G engendré par w_1 et w_2.
a) Quelles sont les dimensions de F et de G?
b) Quelle est la dimension de $F \cap F$?

4.9 Le vecteur $x = (0, 1, 11, -11)$ appartient-il au sous-espace vectoriel de $\mathbb{R}^4$, espace vectoriel sur $\mathbb{R}$, engendré par $a = (2, -1, 3, 7)$ et $b = (1, 0, 7, -2)$?

4.10 Trouver α, β pour que $x = (\alpha, \beta, 31, 12)$ appartienne au sous-espace vectoriel de $\mathbb{R}^4$, engendré par $a = (3, -2, 1, 6)$ et $b = (4, 7, -14, 3)$.

4.11 On considère dans E, espace vectoriel sur $\mathbb{R}$, le sous-espace F engendré par le système de vecteurs $S = \{x_1, \ldots, x_p\}$. On appelle S' le système de vecteurs obtenu en remplaçant dans S le *seul vecteur* x_i par $x_i' = \alpha_1 x_1 + \ldots + \alpha_p x_p$ où $\alpha_1 \ldots \alpha_p$ sont des nombres réels tels que $\alpha_i \neq 0$. Démontrer que F est aussi engendré par S'.

4.12 Dans E espace vectoriel de dimension 3 sur $\mathbb{R}$ de base (e_1, e_2, e_3), on considère les vecteurs

$$a_1 = \alpha_{11} e_1 \quad , \quad a_2 = \alpha_{21} e_1 + \alpha_{22} e_2 \quad , \quad a_3 = \alpha_{31} e_1 + \alpha_{32} e_2 + \alpha_{33} e_3,$$

où les α_{ij} sont des nombres réels tels que le produit $\alpha_{11}\,\alpha_{22}\,\alpha_{33}$ soit *non nul*.
Démontrer que (a_1, a_2, a_3) est une base de E.

4.13 Dans $\mathbb{R}^3$, espace vectoriel sur $\mathbb{R}$, on considère les vecteurs

$$a_1 = (2, 3, 5) \qquad a_2 = (-1, 2, -3) \qquad a_3 = (4, -3, 8).$$

a) Choisir des réels α_1, $\alpha_2 \neq 0$, β_1, $\beta_3 \neq 0$ de manière que la première coordonnée de $a'_2 = \alpha_1 a_1 + \alpha_2 a_2$ et de $a'_3 = \beta_1 a_1 + \beta_3 a_3$ soit nulle.
b) Choisir des réels γ_2, $\gamma_3 \neq 0$ de manière que la deuxième coordonnée de $a''_3 = \gamma_2 a'_2 + \gamma_3 a'_3$ soit nulle.
c) Démontrer que a_1, a'_2, a''_3 sont indépendants (appliquer ex. 4.12).
En déduire que a_1, a_2, a_3 sont indépendants (appliquer ex. 4.11).

4.14 Dans $\mathbb{R}^3$ on considère les vecteurs a_1, a_2, a_3 de l'exercice 4.13. Calculer les coordonnées de $x = (-4, 17, 10)$ par rapport à la base (a_1, a_2, a_3). (Appliquer la méthode de l'exercice 4.13 aux vecteurs a_1, a_2, a_3, x).

4.15 *a*) Démontrer que l'ensemble des vecteurs (x_1, x_2, x_3, x_4) de l'espace vectoriel $\mathbb{R}_4$, vérifiant $x_1 + x_2 + x_3 + x_4 = 0$ est un sous-espace F de $\mathbb{R}^4$.
b) Quelle est la dimension de F? (On considérera les vecteurs $a_1 = (1, 0, 0, -1)$, $a_2 = (0, 1, 0, -1$, $a_3 = (0, 0, 1, -1)$).

4.16 *a*) Démontrer que l'ensemble des vecteurs (x_1, x_2, x_3, x_4) de l'espace vectoriel $\mathbb{R}^4$, vérifiant $x_3 = 2x_1 - x_2$ et $x_4 = x_1 + 3x_2$ est un sous-espace vectoriel F de $\mathbb{R}^4$.
b) Quelle est la dimension de F?

4.17 *On considère l'énoncé $\mathcal{P}(n)$ suivant ($n \geqslant 1$) :
« Quelles que soient les suites réelles $(\alpha_k)_{0 \leqslant k \leqslant n}$ et $(\beta_k)_{1 \leqslant k \leqslant n}$ l'identité

(1) $\qquad (\forall x \in \mathbb{R}) \quad \alpha_0 + \alpha_1 \cos x + \beta_1 \sin x + \ldots + \alpha_n \cos nx + \beta_n \sin nx = 0$

implique $\qquad \alpha_0 = \alpha_1 = \ldots = \alpha_n = \beta_1 = \ldots = \beta_n = 0$ ».

a) Démontrer que l'on a $\mathcal{P}(1)$ $\left(\text{On pourra faire successivement } x = 0,\ x = \pi,\ x = \frac{\pi}{2}\right)$.

b) Démontrer que, pour tout k tel que $2 \leqslant k \leqslant n$, $\mathcal{P}(k-1)$ implique $\mathcal{P}(k)$. (On dérivera deux fois l'identité (1) écrite pour $n = k$, ce qui donnera une identité (2); une combinaison linéaire de (1) et (2) permettra d'éliminer à la fois cos kx et sin kx).
c) Soit E l'ensemble des fonctions numériques définies pour tout x par

$$F(x) = \sum_{k=0}^{n} \alpha_k \cos kx + \sum_{k=1}^{n} \beta_k \sin kx,$$

où $\alpha_0, \ldots, \alpha_n, \ldots, \beta_1, \ldots, \beta_n$ sont des réels quelconques. Démontrer que E est un sous-espace vectoriel de l'espace vectoriel sur $\mathbb{R}$ $(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \bullet)$. Quelle est la dimension de E?

4.18 Soit f l'homomorphisme de $\mathcal{V}_2$, espace vectoriel sur $\mathbb{R}$, dans lui-même défini par

$$f(\vec{i}) = 2\vec{i} + 3\vec{j} \quad , \quad f(\vec{j}) = -3\vec{i} - 4\vec{j},$$

$(\vec{i}, \vec{j})$ étant une base de $\mathcal{V}_2$. Pour tout vecteur $\vec{v}$ de $\mathcal{V}_2$, on pose

$$\vec{v} = x\vec{i} + y\vec{j}, \qquad \vec{v}' = f(\vec{v}) = x'\vec{i} + y'\vec{j}.$$

a) Déterminer la matrice A de f dans la base $(\vec{i}, \vec{j})$.
Calculer x', y' en fonction de x, y.
b) Calculer x, y en fonction de x', y'. En déduire que f est un isomorphisme de $\mathcal{V}_2$ sur $\mathcal{V}_2$. Calculer A^{-1}.

c) Quelle est la droite vectorielle image par f de la droite vectorielle de vecteur directeur $\vec{i} - \vec{j}$? Quelle est la droite vectorielle dont l'image par f est la droite vectorielle de vecteur directeur $\vec{i} + \vec{j}$?

4.19 Soit $(\vec{i}, \vec{j})$ une base de $\mathcal{V}_2$, espace vectoriel sur $\mathbb{R}$. On considère l'homomorphisme f de $\mathcal{V}_2$ dans $\mathcal{V}_2$ dont la matrice relativement à la base $(\vec{i}, \vec{j})$ est $A = \begin{pmatrix} 2 & -1 \\ 4 & 3 \end{pmatrix}$.

a) On pose $i' = 2(\vec{i} + \vec{j})$ et $\vec{j'} = 2(\vec{i} - \vec{j})$; démontrer que $(\vec{i'}, \vec{j'})$ est une base de $\mathcal{V}_2$.

b) Calculer $f(\vec{i'})$ et $f(\vec{j'})$ en fonction de $\vec{i}, \vec{j}$ puis en fonction de $\vec{i'}$ et $\vec{j'}$. En déduire la matrice de f dans la base $(\vec{i'}, \vec{j'})$.

4.20 Dans l'ensemble $\mathcal{M}_2$ des matrices réelles carrées d'ordre 2 on considère la relation $\mathcal{R}$ suivante : « On a $\mathcal{R}$ (A, B) si et seulement s'il existe P inversible de $\mathcal{M}_2$ telle que $B = P^{-1} AP$ ».
Démontrer que $\mathcal{R}$ est une relation d'équivalence.

4.21* Soit $(\vec{i}, \vec{j})$ et $(\vec{i'}, \vec{j'})$ deux bases de l'espace vectoriel $\mathcal{V}_2$ sur $\mathbb{R}$, telles que

$$\vec{i'} = \alpha \vec{i} + \beta \vec{j}, \qquad \vec{j'} = \gamma \vec{i} + \delta \vec{j}.$$

On pose $P = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$.

a) Démontrer que P est la matrice de l'application identique e de $\mathcal{V}_2$ rapporté à la base $(\vec{i'}, \vec{j'})$ sur $\mathcal{V}_2$ rapporté à la base $(\vec{i}, \vec{j})$. (On remarquera que

$$\vec{i'} = e(\vec{i'}) = \alpha \vec{i} + \beta \vec{j} \quad \text{et} \quad \vec{j'} = e(\vec{j'}) = \gamma \vec{i} + \delta \vec{j}).$$

Quelle est la matrice de e, application identique de $\mathcal{V}_2$ rapporté à la base $(\vec{i}, \vec{j})$ sur $\mathcal{V}_2$ rapporté à la base (i', j')?

b) On considère un homomorphisme f de $\mathcal{V}_2$ dans $\mathcal{V}_2$ et on désigne par A sa matrice dans la base $(\vec{i}, \vec{j})$ et par A' sa matrice dans la base $(\vec{i'}, \vec{j'})$. En utilisant le schéma

$$\underset{(\vec{i'}, \vec{j'})}{\mathcal{V}_2} \xrightarrow{e} \underset{(\vec{i}, \vec{j})}{\mathcal{V}_2} \xrightarrow{f} \underset{(\vec{i}, \vec{j})}{\mathcal{V}_2} \xrightarrow{e} \underset{(\vec{i'}, \vec{j'})}{\mathcal{V}_2}$$

démontrer que $A' = P^{-1} AP$.

c) Donner une interprétation des classes d'équivalence, modulo $\mathcal{R}$, pour la relation étudiée à l'exercice 4.20).

4.22 On donne les matrices $A = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}$ et $B = \begin{pmatrix} 0 & -2 \\ 1 & 0 \end{pmatrix}$.

a) Calculer les matrices AB, BA, A^2, B^2, A^2B^2, $(AB)^2$.

b) Démontrer que les matrices A et B sont inversibles.
Calculer A^{-1}, B^{-1}, $(AB)^{-1}$, $B^{-1}A^{-1}$.

4.23 *a*) On donne la matrice $A = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$. Démontrer qu'il existe deux réels α et β tels que $A^2 + \alpha A + \beta I_2 = 0$.

b) Même question pour la matrice $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ où a, b, c, d sont quatre nombres réels quelconques donnés. (On pourra distinguer deux cas : b ou c non nul et $b = c = 0$).

4.24 On munit l'ensemble $\mathcal{M}_2$ des matrices carrées réelles d'ordre 2 de l'addition des matrices et de la multiplication externe, par un réel, suivante :

$$\lambda \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} \lambda a & \lambda c \\ \lambda b & \lambda d \end{pmatrix}$$

a) Démontrer que $(\mathcal{M}_2, +, \bullet)$ est un espace vectoriel sur $\mathbb{R}$.

b) Quelle est la dimension de cet espace vectoriel? On considérera les matrices

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

4.25 On considère l'ensemble E des matrices de la forme $M(a, b) = \begin{pmatrix} a+b & a+3b \\ a-2b & a-b \end{pmatrix}$ où a et b sont deux nombres réels quelconques.

a) Démontrer que E est un sous-espace vectoriel de $(\mathcal{M}_2, +, \bullet)$ (cf. ex. 4.24).

b) Quelle est la dimension de E? (On montrera qu'il existe deux matrices A et B ne dépendant pas de a et b telles que $M(a, b) = aA + bB$).

4.26 On considère l'ensemble E des matrices de la forme $M(a, b, c) = \begin{pmatrix} a+b & b-c \\ b+c & a+c \end{pmatrix}$ où a, b, c sont des réels quelconques.

a) Démontrer que E est un sous-espace vectoriel de $\mathcal{M}_2$.

b) Quelle est la dimension de E? (cf. ex. 4.25).

4.27 On considère les matrices A et B définies par

$$A = \begin{pmatrix} a & 0 \\ b & a \end{pmatrix} = a\,I_2 + B$$

où a et b sont deux nombres réels.

a) Calculer $B^2 \ldots B^n$ ($n \in \mathbb{N}^*$).

b) Dire pourquoi l'on peut appliquer la formule du binôme aux deux matrices aI_2 et B. Calculer A^n pour tout $n \in \mathbb{N}^*$.

4.28 On considère la matrice A définie par

$$A = \begin{pmatrix} x & 0 \\ z & y \end{pmatrix}$$

où x, y, z sont des nombres réels donnés.

Calculer A^n ($n \in \mathbb{N}^*$); on distinguera les deux cas :

1. $x = y$: appliquer l'exercice 4.27.
2. $x \neq y$: calculer d'abord A^2 et A^3 en introduisant $x^2 - y^2$ puis $x^3 - y^3$.

4.29 Dans quel cas la matrice A de l'exercice n° 4.28 est-elle inversible?
Dans ce cas calculer $A^{-1}, A^{-2}, \ldots A^{-n}$ ($n \in \mathbb{N}^*$).

4.30 On considère l'ensemble E des matrices de la forme $\begin{pmatrix} a & 0 \\ a' & a \end{pmatrix}$ où a et a' sont deux nombres réels quelconques.

a) Démontrer que $(E, +, \times)$ est un sous-anneau de l'anneau $\mathcal{M}_2$.

b) Démontrer que l'anneau $(E, +, \times)$ est isomorphe à l'anneau $(D, +, \times)$ étudié à l'exercice 3.27 (chap. 3).

Écrire sous la forme $x + iy$ les nombres complexes suivants (ex. 31 à 40) :

4.31 $\dfrac{1+i}{i}$.

4.32 $\dfrac{i-4}{2i}$.

4.33 $\dfrac{3+4i}{5-7i}$.

4.34 $\dfrac{4-3i}{i-1}$.

4.35 $\dfrac{7i}{2-i}$.

4.36 $\dfrac{3-i}{3+4i}$.

4.37 $\dfrac{(2+i)(3-i)}{4i}$.

4.38 $\dfrac{5-3i}{(4-i)(1+3i)}$.

4.39 $\dfrac{(5+2i)(2-3i)}{(i-3)(3i-4)}$.

4.40 $\dfrac{(8-3i)(i-4)}{(2i-5)(3+7i)}$.

4.41 Déterminer la partie réelle, la partie imaginaire, le module et l'argument du nombre complexe :

$$z = \frac{(1+i)^3}{(1+i\sqrt{3})^4}.$$

4.42 On donne deux nombres réels a et θ. Calculer le module et l'argument du nombre complexe :

$$z = a\,\frac{(1 + i\ \mathrm{tg}\ \theta)^2}{1 + \mathrm{tg}^2\,\theta}.$$

4.43 Soit les nombres complexes : $z_1 = \dfrac{1 + i\sqrt{3}}{1 - i\sqrt{3}}$ et $z_2 = \dfrac{i}{2i\sqrt{3} - 2}$.

Calculer : $z_1 + z_2$, $z_1 . z_2$, $\dfrac{z_1}{z_2}$, $(z_1)^6 . (z_2)^{12}$ et $\dfrac{(z_1)^8}{(z_2)^3}$.

Expliciter z_1, z_2 et tous les résultats sous la forme algébrique la plus simple.

4.44 Étant donné le nombre complexe $z = 1 + i\sqrt{3}$, démontrer que les images dans le plan complexe des nombres z, $-z$, z^2, $\dfrac{2}{z}$ sont cocycliques.

4.45 Soit z le nombre complexe de module 1 et d'argument α.
Calculer, en fonction de α, le module et l'argument du nombre

$$Z = 1 + z + z^2.$$

4.46 Démontrer que, quels que soient les nombres complexes z et z' de module 1 vérifiant $zz' + 1 = 0$, le nombre

$$Z = \frac{z + z'}{1 + zz'}$$

est réel. (On remarquera que Z est réel si et seulement si $Z - \overline{Z} = 0$).

4.47 On considère le nombre complexe $u = 2 - 2i\sqrt{3}$.
1° Mettre u sous forme trigonométrique et en déduire tous les complexes Z tels que $Z^4 = u$.
2° Déterminer, par la méthode algébrique, les nombres complexes X tels que $X^2 = u$, puis les nombres complexes Z tels que $Z^4 = u$.

3° En déduire des expressions de $\sin\dfrac{11\pi}{12}$ et de $\cos\dfrac{11\pi}{12}$ sous forme de radicaux simples.

4.48 Calculer le module et l'argument du nombre complexe :

$$z = \frac{4}{1 + i\sqrt{3}}.$$

Calculer, de deux façons différentes les racines carrées de ce nombre.

4.49 Calculer le module et l'argument du nombre complexe :

$$Z = \frac{1 - \cos\theta + i\sin\theta}{1 + \cos\theta - i\sin\theta} \quad (\theta \text{ vérifie } \pi < \theta < 2\pi).$$

Quelles sont les racines carrées de Z?

4.50 Calculer les racines cubiques du nombre complexe :

$$Z = \frac{1 + i\ \mathrm{tg}\ \theta}{1 - i\ \mathrm{tg}\ \theta}.$$

4.51 Déterminer les racines cubiques du nombre complexe :

$$4\sqrt{2}\,(1 + i).$$

4.52 Déterminer les racines quatrièmes du nombre complexe :

$$z = 8\sqrt{2}\,(-1 - i).$$

4.53 Déterminer les racines cinquièmes du nombre complexe :

$$z = 32\,i.$$

4.54 Déterminer les racines sixièmes du nombre complexe :

$$z = 32\,(i - \sqrt{3}).$$

4.55 Résoudre, dans le corps des nombres complexes, l'équation suivante :

$$z^4 + 6\,z^2 + 25 = 0.$$

4.56 Résoudre, dans le corps des complexes, l'équation suivante :

$$z^4 + 4\,z^2 - 77 = 0.$$

4.57 Résoudre, dans le corps des nombres complexes, l'équation suivante :

$$z^2 + 18\,z + 1\,681 = 0.$$

Déterminer les racines carrées de ses racines.

4.58 Résoudre, dans le corps des nombres complexes, l'équation suivante :

$$(1 - i)\,x^2 - 2\,x - (11 + 3\,i) = 0.$$

4.59 Résoudre, dans le corps des complexes, l'équation :

$$z^2 - (5 - i)\,z + 8 - i = 0.$$

4.60 Résoudre, dans le corps des nombres complexes, l'équation :

$$z^2 + (i - 1)\,(\sqrt{3} - 3)\,z - 12\,i = 0.$$

Calculer le module et l'argument des racines.

4.61 Résoudre, dans le corps des nombres complexes, l'équation :

$$z^2 - 4\,(1 - i)\,z + 2\,(4 - i) = 0.$$

Déterminer le module et l'argument des racines de cette équation.

4.62 Résoudre, dans le corps des nombres complexes, l'équation suivante :

$$z^2 - 2\,z + 4 = 0.$$

Calculer le module, l'argument, le carré et le cube de ses racines.

4.63 Résoudre, dans le corps $\mathbb{C}$, l'équation :

$$\left(\frac{z - i}{z + i}\right)^3 + \left(\frac{z - i}{z + i}\right)^2 + \left(\frac{z - i}{z + i}\right) + 1 = 0$$

4.64 Résoudre, dans le corps des nombres complexes, l'équation :

$$z^2 - (5 + 4\,i\,\sqrt{3})\,z + 9 = 0.$$

On appellera z' la racine ayant le plus grand module.

Calculer le module et l'argument de chacune des racines z' et z'', ainsi que le rapport $\frac{z'}{z''}$.

4.65 Résoudre l'équation :

$$(1 + i)\,z^2 - 2\,i\,(a + 1)\,z + (i - 1)\,(a^2 + 1) = 0,$$

où z est l'inconnue complexe et a un paramètre complexe.

4.66 On considère l'équation en Z à coefficients complexes :

$$Z^3 - (3 + 4\,i)\,Z^2 - 4\,(1 - 3\,i)\,Z + 12 = 0.$$

Montrer qu'elle admet une racine réelle, a, dont on calculera la valeur numérique. Résoudre l'équation dans $\mathbb{C}$.

4.67 Résoudre, dans le corps $\mathbb{C}$ des nombres complexes, l'équation :

$$3z^4 + 2z^2 + 1 = 0.$$

Mettre le polynôme $P(z) = 3z^4 + 2z^2 + 1$ sous forme d'un produit de deux trinômes du second degré à coefficients réels.

4.68 Soit le polynôme :

$$P(x) = x^4 + 4x^3 + 8x^2 + 4x + 7.$$

Sachant que i et $-i$ sont racines de l'équation $P(x) = 0$, mettre $P(x)$ sous la forme d'un produit de deux polynômes du second degré à coefficients réels et calculer les autres racines, réelles ou complexes, de l'équation $P(x) = 0$.

4.69 1° Démontrer que le polynôme :

$$Z^2 + 2(2 + i)Z + 3 + 4i,$$

où Z est un nombre complexe, est le carré d'un polynôme du premier degré.

2° On considère, sur le corps des complexes, l'équation en U

$$(E) \qquad U^2 - 2(Z + 4)U + 2Z^2 + 2(6 + i)Z + 19 + 4i = 0,$$

où Z est un paramètre appartenant lui-même à l'ensemble des complexes.

a) Déterminer Z pour que cette équation ait une racine double.

b) Déterminer les deux solutions de (E) dans le cas général.

c) Déterminer l'ensemble des Z tels que Z soit lui-même une des solutions de l'équation (E).

4.70 Résoudre et discuter l'équation :

$$(E) \qquad 2Z^2(1 + \cos 2\theta) - 2Z \sin 2\theta + 1 = 0,$$

où θ désigne un paramètre réel donné tel que $0 \leqslant \theta \leqslant \pi$, et où Z représente l'inconnue appartenant au corps des nombres complexes.

Quel est, dans un plan rapporté à un repère orthonormé, l'ensemble des points images des solutions quand θ varie sur $[0, \pi]$?

4.71 Quel est, dans le plan, l'ensemble des images M de tous les nombres complexes z tels que $z + \frac{4}{z}$ soit réel?

Résoudre, dans l'ensemble $\mathbb{C}$ des nombres complexes, les équations

$$(1) \quad z + \frac{4}{z} = 5 \qquad (2) \quad z + \frac{4}{z} = 2.$$

Vérifier que les images de leurs racines appartiennent à l'ensemble trouvé.

4.72 Déterminer le nombre complexe z tel que

$$z.\bar{z} + 3(z - \bar{z}) = 13 + 18i.$$

4.73 Soit z un nombre complexe, $\bar{z}$ son complexe conjugué, $|z|$ son module. Quel est l'ensemble des points M du plan dont l'affixe z vérifie

$$z + \bar{z} = |z|?$$

Représenter cet ensemble.

4.74 Soit $Z = \frac{1 - iz}{1 + iz}$. On pose $z = x + iy$.

a) Déterminer une condition que doivent vérifier x et y pour que Z soit réel. Quel est alors l'ensemble des points m d'affixe z?

b) Déterminer une condition que doivent vérifier x et y pour que Z soit imaginaire pur. Quel est alors l'ensemble des points m d'affixe z?

4.75 Déterminer le nombre complexe z tel que les complexes z, $\frac{1}{z}$, $1 - z$ aient le même module.

4.76 Le nombre complexe z a pour image M dans le plan complexe.
On considère le nombre complexe :

$$z = \frac{z - i}{z + i}.$$

Quel est l'ensemble des points M tels que Z soit réel?
Quel est l'ensemble des points M tels que Z soit imaginaire pur?

4.77 Soit le nombre complexe $z = x + iy$ et le nombre $Z = \frac{z + 4i}{z - 4i}$.

Quelle relation doit-il exister entre x et y pour que Z soit réel?
Quelle relation doit-il exister entre x et y pour que Z soit imaginaire pur?

4.78 Soit le nombre complexe $z = x + iy$, affixe d'un point M (distinct de l'origine O) dans le plan complexe.

On considère le nombre complexe z' défini par $z' = \frac{1 + z}{z}$.

Calculer la partie réelle et la partie imaginaire de z'.
Quel est l'ensemble des points M pour lesquels z' est réel?
Quel est l'ensemble des points M tels que z' soit imaginaire pur? Construire cet ensemble.

4.79 Soit un nombre complexe $z = x + iy$, M son image dans le plan complexe. On considère le nombre complexe Z défini, pour $z \neq 0$ par

$$Z = \frac{1}{2}\left(z^2 - \frac{1}{z^2}\right).$$

a) Calculer la partie réelle et la partie imaginaire de Z en fonction de x et y.

b) Quel est l'ensemble des points M tels que Z soit réel?

c) Quel est l'ensemble des points M tels que Z soit imaginaire pur?

4.80 Soit un nombre complexe $z = x + iy$.
Exprimer les nombres complexes z^2 et $1 - z$ au moyen de x et de y.
Quelle relation doit-il exister entre x et y pour que le module de z soit égal au module de z^2?
Cette condition étant remplie, déterminer x et y pour que le module commun à z et z^2 soit égal au module de $1 - z$.
Représenter alors les nombres complexes z correspondants dans le plan complexe. Quel est l'argument de z?

4.81 A tout nombre complexe $z = x + iy$, on associe un point M d'affixe z du plan complexe. Au nombre complexe $a = 10 + 6i$, on associe le point A.

1° Déterminer l'ensemble E_1 des points M tels que le produit $z(z - a)$ soit un nombre réel.

2° Déterminer l'ensemble des points M tels que le produit $z(z - a)$ soit imaginaire pur. On appellera E_2 cet ensemble.

3° Déterminer l'intersection de E_1 et E_2, et démontrer qu'en chacun des points de cette intersection, les tangentes à E_1 et E_2 sont perpendiculaires.

4.82 1° Déterminer dans le plan complexe l'ensemble (L) des points M d'affixe z satisfaisant à la condition :

(1) $\arg z + \arg(z - 1) = \frac{\pi}{2}$.

2° On impose au nombre complexe z de satisfaire à la condition (1) et, en outre, à la condition :

(2) $\arg z - \arg(z - 1) = \theta \quad ; \quad -\pi \leqslant \theta \leqslant \pi$.

Discuter l'existence de z suivant les valeurs de θ; donner, quand il existe, son expression en fonction de θ.

4.83 Dans le plan complexe, on considère les points :
m d'affixe $z = x + iy$,

M d'affixe $Z = X + iY = \dfrac{z+1}{z-1}$,

A d'affixe $+1$,
B d'affixe -1.
On appelle T l'application du plan complexe dans lui-même, qui, au point m fait correspondre le point M.

1° Démontrer que T est involutive.

2° Quel est l'ensemble des points m pour que $|Z| = \sqrt{2}$?

3° Quel est l'ensemble des points m tels que l'argument de Z soit égal à $-\dfrac{\pi}{4} + 2k\pi$?

4° Calculer X et Y en fonction de x et y, puis x et y en fonction de X et Y. Quel est l'ensemble des points M lorsque m décrit le cercle d'équation

$$x^2 + y^2 = 1?$$

Quel est l'ensemble des points M lorsque m décrit la droite d'équation $y = 2$?

4.84 La transformation ponctuelle T associe au point M d'affixe z, dans le plan complexe privé du point A $(+1, 0)$, le point M′ d'affixe z' :

$$z' = \frac{Z - 1 + i}{z - 1}.$$

Montrer que T est égale à sa transformation réciproque; donner le module et l'argument de ses points invariants.

4.85 Dans le plan complexe, on considère les points : A d'affixe 2, M d'affixe $5 + 2i$ et (L) la droite perpendiculaire en A à la droite AM.

1° Soit N le symétrique du point M par rapport au point A; soit M_1 et M_2 les points de (L) tels que :

$$\|\overrightarrow{AM_1}\| = \|\overrightarrow{AM_2}\| = \|\overrightarrow{AM}\|.$$

Calculer les affixes n, m_1, m_2 des trois points N, M_1, M_2.

2° Soit M′ le point du plan défini par :

$$\|\overrightarrow{AM'}\| = 2\|\overrightarrow{AM}\| \quad \text{et} \quad (\overrightarrow{AM}, \overrightarrow{AM'}) = \left(\frac{4\pi}{3}\right).$$

a) Calculer l'affixe, m', du point M′.

b) Calculer l'affixe, n', du point N′ symétrique du point M′ par rapport à la droite (L).

4.86 Dans le plan complexe, le point M est l'image du nombre complexe :

$$Z_M = \cos\theta + i\sin\theta, \quad \text{avec} \quad \theta \in]0, \pi[.$$

1° Quel est l'ensemble des points M?
Soit N le point d'affixe Z_N tel que : $Z_N = 1 + Z_M$.
Quel est l'ensemble des points N quand θ vérifie la condition $\theta \in]0, \pi[$?
2° Trouver le module et l'argument de

$$Z_R = i\frac{1 + Z_M}{1 - Z_M}, \quad \theta \in]0, \pi[.$$

Déterminer l'ensemble des points R images de Z_R.

4.87 1° Soit le nombre complexe $z_0 = \sqrt{2}(1 + i)$. Déterminer les modules et les arguments de z_0 et de $\dfrac{1}{z_0}$. Dans le plan complexe, représenter les points I et J, d'affixes respectives z_0 et $\dfrac{1}{z_0}$.

2° Soit M un point du plan, d'affixe $z \neq 0$, et soit N le point d'affixe $\dfrac{1}{z}$. Déterminer, en fonction de z l'affixe Z du barycentre P des points M et N affectés respectivement des coefficients 2 et 1.

Déterminer la position P du point P_0 quand $z = z_0$. Calculer z pour que P soit le point d'affixe $\frac{1}{3}$.

3° Montrer que les coordonnées (x, y) du point P peuvent se mettre sous la forme :

$$x = \frac{1}{3}\left(2r + \frac{1}{r}\right)\cos\theta \quad \text{et} \quad y = \frac{1}{3}\left(2r - \frac{1}{r}\right)\sin\theta,$$

où r et θ désignent le module et l'argument de z.

4° L'ensemble des points M étant le cercle de centre O et de rayon $\frac{\sqrt{2}}{2}$, quel est l'ensemble des points P correspondants?

4.88 On donne un nombre réel strictement positif, a, et l'on considère l'application du plan complexe dans lui-même qui, au point m d'affixe z ($z \neq 0$) associe le point M d'affixe

$$Z = \frac{3z^2 - a^2}{2z}.$$

1° On pose $z = \rho(\cos\theta + i\sin\theta)$ $(\rho > 0)$,

et $Z = X + iY$ (X et Y réels). Calculer X et Y en fonction de ρ et θ.

2° Quels sont les points invariants de la transformation?

4.89 Le plan est rapporté au repère orthonormé $(O, \vec{i}, \vec{j})$.

On considère les deux points A et B d'affixes respectives $1 - i$ et $\sqrt{3} + i$. Calculer les affixes z des points C pour lesquels le triangle ABC est

a) rectangle isocèle, l'angle droit étant en B (deux cas possibles);

b) rectangle isocèle, l'angle droit étant en C (deux cas possibles);

c) équilatéral (deux cas possibles).

4.90 On considère l'application du plan complexe dans lui-même, qui, au point m d'affixe z ($z = x + iy$, $z \neq 0$) associe le point M d'affixe Z définie par :

$$Z = X + iY = \frac{1}{2}\left(z + \frac{1}{z}\right).$$

1° Quel est le transformé du point a d'affixe $1 + 2i$? De quels points le point $B\left(\frac{1}{2}, 0\right)$ est-il le transformé? Quels sont les points invariants de la transformation? La transformation est-elle injective?

2° Calculer les coordonnées X et Y de M en fonction de x et y.
Déterminer l'ensemble des points m tels que Z soit réel.

4.91 Au point m d'affixe z du plan complexe, on fait correspondre le point M d'affixe Z telle que

$$Z = \frac{z - 1}{z + 2i}.$$

Si on pose : $z = x + iy$, calculer Z en fonction de x et y.
Déterminer l'ensemble des points m tels que Z soit réel et l'ensemble des points m tels que Z soit imaginaire pur. Représenter ces ensembles dans le plan complexe.

4.92 Dans le plan complexe rapporté à un repère orthonormé le point M a pour affixe $z = x + iy$
On donne les nombres réels $a > 0$, $k > 0$ et $k \neq 1$, et α vérifiant $0 < \alpha < \pi$.

a) Démontrer que l'ensemble des points M tels que

$$\left|\frac{z - a}{z + a}\right| = k$$

est un cercle dont on donnera l'équation. Trouver son centre et son rayon en fonction de a et k.

b) Démontrer que l'ensemble des points M tels que

$$\arg\frac{z - a}{z + a} \equiv \alpha \pmod{\pi}$$

est un cercle dont on donnera l'équation. Trouver son centre et son rayon en fonction de a et α.

Reconnaître l'ensemble de points tels que $\arg \dfrac{z-a}{z+a} \equiv \alpha \pmod{2\pi}$.

4.93* Dans le plan complexe, soit le point A d'affixe a et le point B, distinct de A, d'affixe b.

1° Construire le point M_1 d'affixe z_1 tel que $\dfrac{z_1 - a}{z_1 - b} = -1$.

2° Construire le point M_2 d'affixe z_2 tel que $\dfrac{z_2 - a}{z_2 - b} = +2$.

3° Construire le point M_3 d'affixe z_3 tel que $\dfrac{z_3 - a}{z_3 - b} = \dfrac{\sqrt{3}}{2} + \dfrac{i}{2}$.

4° Construire le point M_4 d'affixe z_4 tel que $\dfrac{z_4 - a}{z_4 - b} = 1 - i$.

(Utiliser les résultats de l'ex. 4.91.)

4.94* On considère l'application f de $\mathbb{C}$ dans $\mathbb{C}$ définie pour tout z par :

$$f(z) = (1 + i)\,z + (i - 1).$$

On lui associe l'application F du plan complexe dans lui-même qui, au point M d'affixe z fait correspondre le point $M' = F(M)$ d'affixe $f(z)$.

1° Les applications f et F sont-elles bijectives?

2° Déterminer l'ensemble des points invariants de F.

3° Quelle est la transformée d'une droite par cette application F?
Déterminer, en particulier, la transformée de la droite d'équation

$$x + 2y - 3 = 0?$$

4° Quelle est la transformée d'un cercle?
Déterminer, en particulier, la transformée du cercle d'équation

$$x^2 + y^2 - 2x + 3y = 0.$$

5° Si A désigne le point invariant de F, déterminer, pour un point M quelconque :

$$\frac{\|\overrightarrow{AM'}\|}{\|\overrightarrow{AM}\|}, \quad \text{angle } (\overrightarrow{AM}, \overrightarrow{AM'}).$$

Quelle remarque peut-on faire?

4.95* Soit l'application de $\mathbb{C} - \{i\}$ dans $\mathbb{C} - \{i\}$ définie par :

$$f(z) = \frac{iz + 2}{z - i}.$$

Dans le plan complexe, on considère le point M d'affixe z, et le point M' d'affixe $f(z)$. On associe ainsi à f une transformation ponctuelle F telle que : $M' = F(M)$. Elle est définie sauf lorsque M est le point I d'affixe i.

1° *a*) Déterminer les points invariants de la transformation F. (On les appellera A et B.)

b) Montrer que f est involutive.

c) Montrer que, si $z = iy$ (avec $y \neq 1$), $f(z)$ s'exprime par $f(z) = iY$ où Y est réel.
Montrer que, si $z = x + i$ (avec $x \neq 0$), $f(z)$ s'exprime par $f(z) = X + i$, où X est réel.
En déduire qu'il existe deux droites dont chacune est globalement invariante (on excepte toujours le point I) dans la transformation F.

2° *a*) Montrer que, pour tout $z \neq i$,

$$|f(z) - i| \cdot |z - i| = 1.$$

Quel est le transformé par F d'un cercle de centre I et de rayon R?

b) Montrer que le transformé par F d'un point dont l'affixe est réelle appartient au cercle ayant pour centre le point H d'affixe $\dfrac{3i}{2}$ et pour rayon $\dfrac{1}{2}$.

3° On considère l'application g de $\mathbb{C}$ dans $\mathbb{C}$ définie par :

$$g(z) = z - i.$$

Soit G la transformation ponctuelle associée. Montrer que g est bijective. On désigne par g^{-1} l'application réciproque de g. Déterminer g^{-1}. Déterminer l'application h telle que l'application f définie au début du problème s'écrive :

$$f = g^{-1} \circ h \circ g.$$

4.96* On considère l'application f de $\mathbb{C}$ dans $\mathbb{C}$ définie pour tout z par :

$$f(z) = (1 + i\sqrt{3})\,\bar{z} + (\sqrt{3} - i).$$

On lui associe l'application F du plan complexe dans lui-même qui, au point M d'affixe z fait correspondre le point $M' = F(M)$ d'affixe $f(z)$.

1° Démontrer que l'application f est bijective.

2° Quel est l'ensemble des points invariants de F?

3° Quelle est la transformée de la droite D d'équation :

$$ux + vy + h = 0,$$

par la transformation F?
Existe-t-il des droites parallèles à leur transformée? confondues avec leur transformée?
Existe-t-il des droites perpendiculaires à leur transformée?
Quelles sont les droites qui font un angle égal à $+\frac{\pi}{3}$ ou $-\frac{\pi}{3}$ avec leur transformée?

4.97* On considère l'application f de $\mathbb{C}^*$ dans $\mathbb{C}^*$ définie pour tout z par :

$$f(z) = \frac{k}{\bar{z}} \quad (k \in \mathbb{R}^*).$$

On lui associe l'application F du plan complexe privé de O dans lui-même, qui, au point M d'affixe z, fait correspondre le point $M' = F(M)$ d'affixe $f(z)$.

1° Démontrer que l'application f est bijective, de même que l'application F.

2° Déterminer l'ensemble des points invariants de la transformation F. Discuter suivant les valeurs de k.

3° Quelle est la transformée de la droite D d'équation : $ux + vy + h = 0$ par la transformation F? Quelles sont les droites globalement invariantes par F?

4° Quel est le transformé du cercle (C) d'équation :

$$x^2 + y^2 - 2ax - 2by + c = 0 \quad (a^2 + b^2 - c \geqslant 0)$$

par la transformation F? Quels sont les cercles globalement invariants par F?

4.98** On considère l'ensemble E des équations du 4e degré, à coefficients réels, de la forme :

(1) $$f(x) = x^4 + 2ax^3 + bx^2 + 2ax + 1 = 0.$$

1° Après avoir divisé $f(x)$ par x^2, poser $x + \frac{1}{x} = u$, et montrer que la nouvelle inconnue u est racine de l'équation :

(2) $$u^2 + 2au + b - 2 = 0.$$

En déduire que l'équation (1) a toujours 4 racines, réelles ou non, distinctes ou non.

2° *a*) En revenant à la forme initiale,

(1) $$x^4 + 2ax^3 + bx^2 + 2ax + 1 = 0,$$

montrer que, si l'équation (1) a une racine complexe, non réelle, x_0, elle a aussi pour racine le nombre conjugué de x_0 et le nombre inverse de x_0.

b) En déduire qu'alors, si le module de x_0 est différent de 1, l'équation (1) a 4 racines complexes, dont on précisera la disposition des images dans le plan complexe. Une telle équation (1) sera dite du type I.

c) Déterminer a et b, sachant que l'équation (1) admet pour racine le nombre $(2 + i)$. Résoudre dans ce cas l'équation (1) et mettre $f(x)$ sous forme d'un produit de deux polynômes de la variable x à coefficients réels.

d) Mêmes questions qu'au § *c*), en supposant maintenant que l'équation (1) admet pour racine le nombre : $\rho(\cos\theta + i\sin\theta)$, ρ et θ étant deux réels tels que :

$$\rho > 1 \quad , \quad 0 < \theta < \pi.$$

3° *a*) Montrer que, si l'équation (1) a une racine complexe, non réelle de module 1, elle a ou bien trois autres racines de module 1 (type II), ou bien deux autres racines réelles et inverses (type III).

b) Montrer que l'équation (1) peut avoir quatre racines réelles (type IV).

c) Représenter, dans le plan complexe, les images des 4 racines de l'équation (1) pour chacun des types II, III, IV.

4° *a*) A chaque élément e de E, on associe le point M de coordonnées (a, b) dans un plan rapporté à un repère orthonormé. M est appelé image de e. Discuter, suivant la position de M, le type de l'équation e.

b) L'équation (1) étant du type I, trouver l'ensemble des points M tels qu'une racine de l'équation e associée ait un module donné ρ ($\rho > 1$).

c) L'équation (1) étant du type III, les images dans le plan complexe de ses quatre racines peuvent-elles être cocycliques?

4.99** On considère l'ensemble E des équations du 4e degré, à coefficients réels, de la forme :

(1) $$f(x) = x^4 - 2ax^2 + b = 0.$$

1° *a*) Montrer que l'équation (1) a toujours 4 racines, réelles ou non, distinctes ou non.

b) Montrer que, si l'équation (1) a une racine complexe x_0, non réelle et non imaginaire pure, elle a aussi pour racine le nombre conjugué de x_0 et le nombre opposé de x_0. On dira alors que l'équation (1) est du type I. Quelle est, dans ce cas, la disposition des images, dans le plan complexe des 4 racines?

c) Résoudre l'équation (1) si

$$a = \rho^2 \cos 2\theta \quad \text{et} \quad b = \rho^4,$$

ρ et θ étant deux nombres réels tels que :

$$\rho > 0 \quad , \quad 0 < \theta < \frac{\pi}{2}.$$

Mettre alors $f(x)$ sous forme d'un produit de deux polynômes de la variable x à coefficients réels.

2° A chaque élément e de E on fait correspondre le point M de coordonnées (a, b) d'un plan rapporté à un repère orthonormé. M est appelé image de e. Discuter, suivant la position du point M, si l'équation (1) est du type I précédent, ou si elle a 4 racines imaginaires pures (type II), ou si deux de ses racines et deux seulement sont imaginaires pures (type III), ou si elle a 4 racines réelles (type IV). Donner la disposition, dans le plan complexe, des images des 4 racines de (1) pour chacun des types II, III, IV.

3° L'équation (1) étant du type (I), trouver l'ensemble des points M :

a) tels que le module d'une racine de (1) soit un nombre donné ρ;

b) tels que l'argument d'une racine de (1) soit un nombre donné θ.

4° L'équation (1) étant du type III, trouver l'ensemble des points M :

a) tels que les côtés du polygone convexe ayant pour sommets les images des racines de (1) aient une longueur donnée l;

b) tels que l'aire de ce polygone soit un nombre donné S;

c) tels que le rayon de son cercle inscrit soit un nombre donné r.

Factoriser les expressions suivantes où x représente un réel quelconque (ex. 100 à 108) :

4.100 $\sin x + \sin 2x + \sin 3x$.

4.101 $\cos x + \cos 2x + \cos 3x$.

4.102 $\sin x + \sin 2x + \sin 3x + \sin 4x$.

4.103 $\cos x + \cos 2x + \cos 3x + \cos 4x$.

4.104 $\sin x - \sin 2x + \sin 3x - \sin 4x$.

4.105 $\cos x - \cos 2x + \cos 3x - \cos 4x$.

4.106 $\sin x - \cos 2x + \sin 3x - \cos 4x$.

4.107 $\sin x + \cos 2x - \sin 3x - \cos 4x$.

4.108 $\sin x + \sin 3x - \sin 5x - \sin 7x$.

Démontrer que, quels que soient les réels vérifiant $x + y + z = \pi$ *on a les égalités suivantes* (ex. 109 à 114) :

4.109 $\sin x + \sin y + \sin z = 4 \cos \frac{x}{2} \cos \frac{y}{2} \cos \frac{z}{2}$.

4.110 $\cos x + \cos y + \cos z = 1 + 4 \sin \frac{x}{2} \sin \frac{y}{2} \sin \frac{z}{2}$.

4.111 $\sin x + \sin y - \sin z = 4 \cos \frac{x}{2} \sin \frac{y}{2} \sin \frac{z}{2}$.

4.112 $\operatorname{tg} x + \operatorname{tg} y + \operatorname{tg} z = \operatorname{tg} x \operatorname{tg} y \operatorname{tg} z$.

4.113 $\operatorname{tg} \frac{y}{2} \operatorname{tg} \frac{z}{2} + \operatorname{tg} \frac{z}{2} \operatorname{tg} \frac{x}{2} + \operatorname{tg} \frac{x}{2} \operatorname{tg} \frac{y}{2} = 1$.

4.114 $\cos 2x + \cos 2y + \cos 2z = -1 - 4 \cos x \cos y \cos z$.

Résoudre les équations suivantes, dans $\mathbb{R}$ (ex. 115 à 118) :

4.115 $\sin 7x - \sin x = \sin 3x$.

4.116 $\sin x + 2 \sin 2x + \sin 3x = 0$.

4.117 $\operatorname{tg} 2x + \operatorname{tg} x = \operatorname{tg} 3x$.

4.118 $\sin x + \sin 3x = \cos x + \cos 3x$.

4.119 Vous verrez en analyse que l'on est amené à poser, quel que soit le réel x,

$$e^{ix} = \cos x + i \sin x.$$

a) A quoi est égal e^{-ix}? Démontrer que, quel que soit le réel x, on a (formules d'EULER)

$$\cos x = \frac{e^{ix} + e^{-ix}}{2} \quad , \quad \sin x = \frac{e^{ix} - e^{-ix}}{2i}.$$

b) Démontrer que, quels que soient x et y réels on a

$$e^{ix} e^{iy} = e^{i(x+y)}.$$

c) Démontrer que, quels que soient x de $\mathbb{R}$ et n de $\mathbb{Z}$ on a

$$(e^{ix})^n = e^{nix}.$$

Soit P *un polynôme à coefficients réels et à 2 variables réelles. Linéariser* P $(\cos x, \sin x)$ *c'est-à-dire trouver des suites réelles* $(\alpha_k)_{0 \leqslant k \leqslant n}$, $(\beta_k)_{0 \leqslant k \leqslant n}$ *telles que*

$$\mathrm{P}(\cos x, \sin x) = \sum_{k=0}^{k=n} (\alpha_k \cos kx + \beta_k \sin kx),$$

pour les fonctions suivantes. (On pourra soit utiliser les formules de transformation de « produits en sommes » soit les formules d'Euler (ex. 4.119).) (Ex. 120 à 123).

4.120 *a*) $\cos^3 x$ *b*) $\sin^3 x$ *c*) $\cos^4 x$ *d*) $\sin^4 x$.

4.121 $\cos^3 x \sin^4 x + \sin^3 x \cos^4 x$.

4.122 $16 \cos^4 x \sin^3 x + 8 \cos^3 x \sin^2 x$.

4.123 $4 \cos^3 x \sin x - 5 \cos x \sin x + 8 \sin^3 x + 4 \cos^2 x$.

Sujets d'étude.

4.124 En utilisant la formule du binôme $(1 + x)^n$ calculer les nombres suivants :

a) $A_0 = C_n^0 + C_n^3 + C_n^6 + \ldots$.

$A_1 = C_n^1 + C_n^4 + C_n^7 + \ldots$.

$A_2 = C_n^2 + C_n^5 + C_n^8 + \ldots$.

(Prendre $x = 1$, $x = j$, $x = j^2$).

b) $B_0 = C_n^0 + C_n^4 + C_n^8 + \ldots$.

$B_1 = C_n^1 + C_n^5 + C_n^9 + \ldots$.

$B_2 = C_n^2 + C_n^6 + C_n^{10} + \ldots$.

$B_3 = C_n^3 + C_n^7 + C_n^{11} + \ldots$.

(Prendre $x = 1$, $x = i$, $x = -1$, $x = -i$).

4.125 En utilisant les formules d'EULER (cf. ex. 4.119) linéariser $\cos^n x$ et $\sin^n x$ (cf. introduction aux exercices 120 à 123).

a) Pour n pair.

b) Pour n impair.

4.126 On appelle suite géométrique de nombres complexes toute suite de nombres complexes (u_n) telle que

$$u_0 = a \quad \text{et,} \quad \text{pour } n \geqslant 1, \quad u_n = aq^n$$

ou a et q sont des nombres complexes donnés.

a) Calculer $\sum_{k=0}^{k=n} u_k$. (On distinguera les cas $q = 1$ et $q \neq 1$).

b) On pose $A = 1 + \cos x + \ldots + \cos nx$, $B = \sin x + \ldots + \sin nx$. Calculer $A + iB$ sous forme trigonométrique. En déduire A et B. (On supposera $x \not\equiv 0 \pmod{2\pi}$).

c) Calculer de même

$$C = \cos a + \cos(a + r) + \ldots + \cos(a + nr)$$
$$S = \sin a + \sin(a + r) + \ldots + \sin(a + nr)$$

a et r étant deux nombres réels donnés. (On supposera $r \not\equiv 0 \pmod{2\pi}$).

4.127 Soit p et q deux nombres complexes avec $q \neq 0$. On considère l'ensemble S des suites (u_n) de nombres complexes vérifiant, pour tout n de $\mathbb{N}$,

$$u_{n+2} + pu_{n+1} + qu_n = 0.$$

a) Démontrer que S muni de l'addition et de la multiplication externe par un complexe suivantes :

$$(u_n) + (v_n) = (u_n + v_n),$$
$$\lambda\,(u_n) = (\lambda\, u_n),$$

est un espace vectoriel sur le corps commutatif $\mathbb{C}$.

b) On considère l'application f de S dans $\mathbb{C} \times \mathbb{C}$ qui à toute suite (u_n) de S associe l'élément (u_0, u_1) de $\mathbb{C} \times \mathbb{C}$. Démontrer que f est un isomorphisme de S sur $\mathbb{C} \times \mathbb{C}$, tous deux espaces vectoriels sur $\mathbb{C}$.

c) Démontrer qu'il existe une suite unique (a_n) de S telle que $a_0 = 1$, $a_1 = 0$ et une suite unique (b_n) de S telle que $b_0 = 0$, $b_1 = 1$. En déduire que pour toute suite (u_n) de S, il existe un couple unique (α, β) de nombres complexes tel que l'on ait, pour tout n, $u_n = \alpha\, a_n + \beta\, b_n$.
Quelle est la dimension de S sur $\mathbb{C}$?

d) Démontrer que si $p^2 - 4q \neq 0$, il y a dans S deux suites linéairement indépendantes de la forme s^n ($s \in \mathbb{C}$). Calculer u_n en fonction de n, u_0, u_1, p, q.

Applications numériques

1° $p = q = -1$, $u_0 = u_1 = 1$ (suite de FIBONACCI, cf. ex. 1.28 du chapitre 1).

2° $p = -2k\cos\varphi$, $q = k^2$, $u_0 = 1$, $u_1 = k\cos\varphi$ (k, φ réels).

e) Si $p^2 - 4q = 0$, il n'y a dans S qu'une seule suite de la forme s^n. Quelle relation vérifie la suite (v_n) définie, pour tout entier naturel n, par $u_n = s^n v_n$? Déduire de cette étude deux suites de S linéairement indépendantes. Calculer u_n en fonction de n, u_0, u_1, p.

4.128 Trouver tous les homomorphismes f du corps $\mathbb{C}$ dans lui-même tels que l'application f soit distincte de l'application nulle et que $f(\mathbb{R}) \subset \mathbb{R}$. (Utiliser l'exercice 3.76).

5| Probabilités.

Vous avez vu en classe de Première des exemples de phénomènes aléatoires et vous avez étudié un premier modèle mathématique de ces phénomènes. Nous allons ici reprendre la question pour construire un modèle plus élaboré et aller plus loin dans les applications. Nous définirons notamment la notion d'espérance mathématique, cas particulier de la notion fondamentale d'intégrale. Comme application nous démontrerons une forme de la loi des grands nombres.

5.1 INTRODUCTION

Si l'on regarde sous un microscope des grains de pollen en suspension dans l'eau, on s'aperçoit qu'ils sont animés d'un mouvement continu et qui paraît totalement désordonné. La vitesse moyenne d'un grain donné pendant une durée d'observation grandit sans cesse et varie énormément en direction lorsque cette durée diminue. Des grains différents ont des trajectoires apparemment très différentes et il est impossible à tout moment et dans n'importe quelle situation de prévoir le comportement ultérieur des grains. Nous sommes en présence d'un phénomène régi par le hasard c'est-à-dire d'un **phénomène aléatoire.** Ce phénomène s'appelle le mouvement brownien du nom du botaniste anglais Brown qui le découvrit en 1828.

Depuis 1900 et surtout depuis 1923 avec NORBERT WIENER, les mathématiciens en ont donné un modèle mathématique très élaboré, qui fait encore l'objet de nombreuses recherches, mais qui utilise certains outils mathématiques très puissants. Nous allons en étudier maintenant une schématisation rudimentaire qui n'est pas encore un modèle mathématique.

Considérons un voyageur qui se déplace dans le réseau plan infini R (fig. 1. p. 266) de la façon suivante : il dispose d'un sac dans lequel sont placées quatre boules marquées des noms des points cardinaux; à l'instant 0 le voyageur est au point(0, 0), à l'instant 1 il tire une boule du sac et se déplace d'une maille dans la direction indiquée par la boule, celle-ci est ensuite remélangée avec les autres; à l'instant 2 il retire une boule du sac et se déplace à nouveau d'une maille dans la direction indiquée et ainsi de suite. Ce voyageur va effectuer un trajet aléatoire dans ce réseau ou encore décrire une **trajectoire** dans R. Une trajectoire peut être considérée comme une application f de $\mathbb{N}$ dans R telle que $f(0) = (0, 0)$. On appellera **espace des trajectoires** l'ensemble Ω de ces applications. Chaque trajectoire $\omega \in \Omega$ est un des résultats possibles de l'expérience aléatoire décrite ci-dessus.

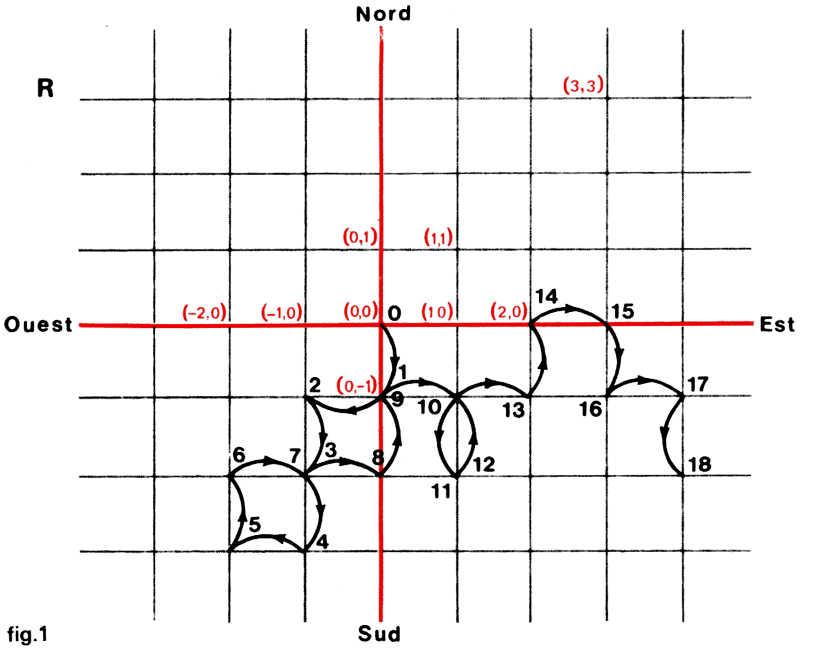


fig.1

Si l'on veut essayer de décrire a priori le voyage qui sera réalisé au cours d'une expérience, on va être naturellement amené à se poser des questions telles que les suivantes : est-il vrai que? Quelle chance a-t-on que?

1° le voyageur repasse certainement tôt ou tard par le point (0, 0);
2° le voyageur repasse une infinité de fois par le point (0, 0);
3° le voyageur passe certainement par tous les points du réseau;
4° le voyageur atteint le point (1, 3) avant le sixième instant;
5° si A et B sont deux sous-ensembles de R, le voyageur atteint A avant d'atteindre B;
6° le voyageur évite le point (3, 3).

Nous dirons que ceci est une liste **d'événements aléatoires.**

Soit E un événement aléatoire on peut toujours lui faire correspondre l'événement **contraire** $\complement E$ qui est réalisé si et seulement si E ne l'est pas; dans l'exemple précédent les contraires de 1° et 6° sont

pour 1° : le voyageur ne repassè jamais par le point (0, 0);
pour 6° : le voyageur passe par le point (3, 3).

Si E et F sont deux événements on peut leur faire correspondre les événements (E ou F) qui est réalisé si et seulement si au moins l'un des deux est réalisé et (E et F) qui est réalisé si et seulement si les deux le sont; ainsi

1° ou 6° : le voyageur repasse par (0, 0) ou évite (3, 3);
1° et 6° : le voyageur repasse par (0, 0) et évite (3, 3).

Pour tout événement E, l'événement (E ou $\complement E$) est un événement forcément réalisé qu'on appelle l'événement **certain**; l'événement (E et $\complement E$) est un événement irréalisable qu'on appelle l'événement **impossible.**

Si on connaît la trajectoire $\omega \in \Omega$ décrite par le voyageur on doit pouvoir dire avec certitude si l'événement E est réalisé ou non. Ainsi la trajectoire dessinée figure 1 et supposée

prolongée vers le Sud-Est ne réalise ni 1° ni 6°. A un événement E on va faire correspondre l'ensemble $\tilde{E}$ des trajectoires qui réalisent E, c'est-à-dire une partie de Ω.

A l'ensemble des événements on va ainsi faire correspondre une partie $\mathcal{B}$ de $\mathcal{P}(\Omega)$. On voit que $\mathcal{B}$ contient l'ensemble Ω qui correspond à l'événement certain, l'ensemble $\varnothing$ qui correspond à l'événement impossible et que si $\tilde{E}$ et $\tilde{F}$ sont deux éléments de $\mathcal{B}$ correspondant aux événements E et F, les ensembles $\complement_\Omega \tilde{E}$, $\tilde{E} \cup \tilde{F}$, $\tilde{E} \cap \tilde{F}$ qui correspondent à $\complement$ E, (E ou F), (E et F) sont aussi dans $\mathcal{B}$.

Maintenant à certains événements il est facile d'associer un nombre compris entre 0 et 1 qui mesure le degré de « chance » qu'on a de voir l'événement se réaliser. Ainsi on accorde volontiers à l'événement {le voyageur est en (0, 1) à l'instant 1} le nombre 1/4, à l'événement certain le nombre 1, à l'événement impossible le nombre 0. Si on accorde à E le nombre a, on accordera $1-a$ à son contraire; si E et F sont deux événements tels que (E et F) soit impossible on accordera à (E ou F) la somme des nombres accordés à E et F.

Quels nombres va-t-on pouvoir accorder aux événements décrits plus haut? Un des objets de la théorie des probabilités est de répondre à cette question dans le cadre d'un modèle mathématique que l'on va décrire maintenant et qui essaie de garder la structure mise en évidence dans l'analyse qui précède. Malheureusement ce modèle qui convient aussi pour les questions de surface, de volume, de distributions d'électricité, ..., ne peut pour le moment être développé que lorsque Ω est un ensemble fini.

I. Espaces de probabilité finis

5. 2 TRIBUS. ESPACES PROBABILISABLES

Définition.

Soit Ω un ensemble on appelle **tribu sur** Ω ou **algèbre de Boole de parties de** Ω un sous-ensemble $\mathcal{B}$ de $\mathcal{P}(\Omega)$ tel que

i) la partie pleine Ω appartient à $\mathcal{B}$;
ii) si $A \in \mathcal{B}$, alors $\complement A \in \mathcal{B}$;
iii) si A et B appartiennent à $\mathcal{B}$, $A \cup B$ appartient à $\mathcal{B}$.

De cette définition nous allons facilement déduire la proposition suivante.

Théorème.

1. Une tribu $\mathcal{B}$ contient la partie vide $\varnothing$.
2. Si $A_1, A_2, \ldots, A_n$ est une suite d'éléments de $\mathcal{B}$, la réunion $A_1 \cup A_2 \ldots \cup A_n$ est élément de $\mathcal{B}$; l'intersection $A_1 \cap A_2 \cap \ldots \cap A_n$ est élément de $\mathcal{B}$.
3. Si $A, B \in \mathcal{B}$, la différence symétrique $A \triangle B$ appartient à $\mathcal{B}$; la différence $A - B$ appartient à $\mathcal{B}$.

Les propriétés 2° et 3° peuvent encore s'exprimer : une tribu $\mathcal{B}$ est fermée pour les opérations de réunion, d'intersection, de différence et de différence symétrique. Tous les ensembles Ω considérés dans la suite sont finis; on ne le rappellera pas systématiquement.

Démonstration : La propriété 1° résulte immédiatement des propriétés i) et ii) de la définition.

Pour démontrer 2° notons tout d'abord que $A_1 \cup A_2 \in \mathcal{B}$ d'après iii) de la définition; raisonnons par récurrence et supposons que $A_1 \cup A_2 \ldots \cup A_{n-1} \in \mathcal{B}$ alors iii) entraîne $(A_1 \cup A_2 \ldots \cup A_{n-1}) \cup A_n \in \mathcal{B}$ ce qui est le résultat désiré. Comme

$$\complement (A_1 \cap A_2 \ldots \cap A_n) = (\complement A_1) \cup (\complement A_2) \ldots \cup (\complement A_n),$$

la 2e assertion de 2° est également vraie d'après ii) et iii) de la définition.
Soit maintenant A, $B \in \mathcal{B}$; comme $A - B = A \cap \complement B$, on a $A - B \in \mathcal{B}$. Comme

$$A \Delta B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A),$$

on a aussi $A \Delta B \in \mathcal{B}$.

EXEMPLES

1. Pour tout ensemble Ω, $\mathcal{T}(\Omega)$ est une tribu sur Ω. L'ensemble $\mathcal{B} = \{\varnothing, \Omega\}$ est une tribu appelée tribu **grossière.**
2. Si Ω a plus d'un point et si A est un sous-ensemble propre de Ω, l'ensemble $\mathcal{B} = \{\varnothing, \Omega, A, \complement A\}$ est une tribu sur Ω.
3. Plus généralement si $(A_1, A_2, \ldots, A_n)$ est une partition π de Ω, l'ensemble $\mathcal{B}$ des sous-ensembles de Ω qui sont de la forme

$$B = A_{i_1} \cup A_{i_2} \ldots \cup A_{i_p}$$

avec $0 \leqslant p \leqslant n$, $i_j \in \{1, 2, \ldots, p\}$ pour $j = 0, 1, \ldots, p$, est une tribu; on obtient l'ensemble $\varnothing$ pour $p = 0$. Ceci peut encore s'exprimer en disant que $\mathcal{B}$ est la tribu des **réunions finies d'ensembles de** π ou que $\mathcal{B}$ est **engendrée** par la partition π. Réciproquement si Ω est de cardinal fini, une tribu $\mathcal{B}$ sur Ω est aussi de cardinal fini. Pour tout $\omega \in \Omega$, l'intersection des ensembles de $\mathcal{B}$ qui contiennent ω est encore un ensemble de $\mathcal{B}$, c'est le plus petit ensemble de B contenant ω. La relation d'équivalence sur Ω définie par : $\omega \sim \omega'$ si et seulement si le plus petit élément de $\mathcal{B}$ contenant ω est aussi le plus petit élément de $\mathcal{B}$ contenant ω' induit une partition π sur Ω. La tribu engendrée par π est égale à $\mathcal{B}$. **Toute tribu sur un ensemble fini est engendrée par une partition.** Les éléments de π sont parfois appelés **constituants indépendants.**

COMPLÉMENTS

1° *Tribu engendrée.* Soit Ω un ensemble et $\mathcal{B}_i$ une famille de tribus sur Ω. L'intersection des tribus $\mathcal{B}_i$ est l'ensemble des parties de Ω qui appartiennent à toutes les tribus $\mathcal{B}_i$; cette intersection est encore une tribu; en effet :
i) Ω appartient à toutes les $\mathcal{B}_i$
ii) Si A appartient à toutes les $\mathcal{B}_i$, $\complement A$ appartient aussi à toutes les $\mathcal{B}_i$;
iii) Si A et B appartiennent à toutes les $\mathcal{B}_i$, $A \cup B$ appartient à toutes les $\mathcal{B}_i$.
Soit maintenant $\mathcal{A}$ une partie non vide de $\mathcal{T}(\Omega)$; la famille des tribus contenant $\mathcal{A}$ n'est pas vide puisque $\mathcal{T}(\Omega)$ est une tribu contenant $\mathcal{A}$. L'intersection de toutes les tribus de cette famille est encore une tribu contenant $\mathcal{A}$ et c'est la **plus petite tribu contenant** $\mathcal{A}$, on l'appelle la tribu **engendrée** par $\mathcal{A}$. Ceci généralise la notion de tribu engendrée par une partition.
2° *Tribu produit* : Soit $\mathcal{B}_1$ et $\mathcal{B}_2$ deux tribus sur des espaces finis Ω_1 et Ω_2; elles sont donc engendrées par des partitions π_1 et π_2. Considérons la partition de $\Omega_1 \times \Omega_2$ constituée par les ensembles

$$A_1 \times A_2 = \{(\omega_1, \omega_2),\ \omega_1 \in A_1,\ \omega_2 \in A_2\}$$

pour $A_1 \in \pi_1$, $A_2 \in \pi_2$. Cette partition engendre une tribu sur $\Omega_1 \times \Omega_2$ appelée **tribu produit** et notée $\mathcal{B}_1 \otimes \mathcal{B}_2$.

Définition.

On appelle **espace probabilisable fini** un couple $(\Omega, \mathcal{B})$ où Ω est un ensemble fini et $\mathcal{B}$ une tribu sur Ω.

L'ensemble Ω s'appelle encore l'ensemble des **épreuves** ou ensemble des **trajectoires** et $\mathcal{B}$ la tribu des **événements.** Pour désigner les éléments de $\mathcal{B}$ nous emploierons indifféremment les mots ensembles et événements.

5. 3 ESPACES DE PROBABILITÉ

a) Définition.

On appelle **probabilité sur l'espace probabilisable fini** $(\Omega, \mathfrak{B})$ une application P de $\mathfrak{B}$ dans [0, 1] telle que

i) $P(\Omega) = 1$;

ii) Si A et B sont deux éléments disjoints de $\mathfrak{B}$ $(A \cap B = \varnothing)$,

$$P(A \cup B) = P(A) + P(B),$$

ce qui s'exprime en disant que P est **additive.**

Voyons quelques *conséquences* de cette définition.

En raisonnant par récurrence comme au paragraphe précédent on voit tout d'abord que si $A_1, \ldots, A_n$ est une suite d'éléments de $\mathfrak{B}$ deux à deux disjoints $(A_i \cap A_j = \varnothing$ si $i \neq j)$ on a

$$P(A_1 \cup A_2 \ldots \cup A_n) = P(A_1) + P(A_2) + \ldots + P(A_n).$$

Pour tout $A \in \mathfrak{B}$, on a $A \cap \complement A = \varnothing$ et $A \cup \complement A = \Omega$; on a donc

$$P(A) + P(\complement A) = P(A \cup \complement A) = P(\Omega) = 1,$$

ce qui entraîne que $P(\complement A) = 1 - P(A)$. En particulier $P(\varnothing) = 1 - P(\Omega) = 0$.

Si A et B sont deux éléments de $\mathfrak{B}$, les ensembles $A - B$ et $A \cap B$ sont disjoints et de réunion A; on a donc

$$P(A) = P(A - B) + P(A \cap B).$$

Si $A \supset B$, $A \cap B = B$, et il résulte de cette formule que P (A) est plus grand que P (B). Si A et B sont quelconques, on a par symétrie

$$P(B) = P(B - A) + P(A \cap B),$$

et en ajoutant les deux formules

$$P(A) + P(B) = P(A - B) + P(B - A) + 2P(A \cap B);$$

comme les parties $A - B$, $B - A$ et $A \cap B$ sont disjointes deux à deux et de réunion $A \cup B$ on obtient

$$P(A) + P(B) = P(A \cup B) + P(A \cap B).$$

Résumons ces propriétés :

Théorème.

Si P est une probabilité sur $(\Omega, \mathfrak{B})$ on a pour $A, B \in \mathfrak{B}$

1. $P(\complement A) = 1 - P(A)$, $P(\varnothing) = 0$;
2. Si $A \subset B$, $P(A) \leqslant P(B)$, ce qui s'exprime en disant que P est une application **croissante.**
3. $P(A \cup B) = P(A) + P(B) - P(A \cap B)$, ce qui s'exprime en disant que P est une application **fortement additive.**

b) Définition.

On appelle **espace de probabilité fini** la donnée d'un triplet $(\Omega, \mathfrak{B}, P)$ où Ω est un ensemble fini, $\mathfrak{B}$ une tribu sur Ω et P une probabilité sur $(\Omega, \mathfrak{B})$.

EXEMPLES

1. Sur une tribu grossière il n'existe qu'une seule probabilité.
2. Si Ω n'est pas réduit à un point et si $\mathcal{B} = \{\Omega, \varnothing, A, \complement A\}$ pour un sous-ensemble propre A de Ω, pour tout $p \in [0, 1]$ on définit une probabilité P sur $(\Omega, \mathcal{B})$ en posant $P(A) = p$, $P(\complement A) = 1 - p = q$. Cet espace de probabilité est un modèle du jeu de pile ou face (avec une pièce truquée si $p \neq 1/2$).
3. Plus généralement si $\mathcal{B}$ est engendrée par une partition $(A_1, A_2, \ldots, A_n)$ on définit une probabilité sur $(\Omega, \mathcal{B})$ en se donnant des nombres $P(A_i) = p_i$ tels que
$$p_1 + p_2 + \ldots + p_n = 1.$$
3. Lorsque $\mathcal{B} = \mathcal{T}(\Omega)$ tous les ensembles ne contenant qu'un seul point sont dans $\mathcal{B}$, ou, ce qui revient au même, $\mathcal{B}$ est engendrée par la partition la plus fine de Ω. Pour définir P il suffit alors de donner $P(\{\omega\})$ pour tout $\omega \in \Omega$. Un cas particulier important est celui où on admet que tous les événements $\{\omega\}$ sont **équi-probables,** c'est-à-dire que l'on pose
$$P(\{\omega\}) = 1/\text{card}\ (\Omega)$$
pour tout $\omega \in \Omega$. La probabilité d'un événement $A \in \mathcal{B}$ est alors donnée par
$$P(A) = \text{card}\ (A)/\text{card}\ (\Omega).$$
Dans toute la suite notamment dans les exercices, la locution **tirer au hasard** signifiera que l'on considère un espace de probabilité de ce type. Soit par exemple à trouver la probabilité d'avoir au moins un as lorsque on « tire au hasard » trois cartes d'un jeu de 52; l'espace de tous les choix possibles de 3 cartes différentes parmi 52, soit encore l'espace des injections de l'ensemble $\{1, 2, 3\}$ dans l'ensemble $\{1, \ldots, 52\}$ a pour cardinal C_{52}^3. L'ensemble des groupes de trois cartes ne contenant aucun as est l'ensemble des injections de $\{1, 2, 3\}$ dans $\{1, \ldots, 48\}$ et a pour cardinal C_{48}^3. La probabilité cherchée est donc égale à
$$1 - \frac{C_{48}^3}{C_{52}^3} = 1 - \frac{48 \times 47 \times 46}{52 \times 51 \times 50} \# 0{,}23$$

COMPLÉMENTS

Probabilité produit. Si $(\Omega_1, \mathcal{B}_1, P_1)$ et $(\Omega_2, \mathcal{B}_2, P_2)$ sont deux espèces de probabilité on va définir une nouvelle probabilité sur $(\Omega_1 \times \Omega_2, \mathcal{B}_1 \otimes \mathcal{B}_2)$ de la manière suivante : on a vu précédemment que $\mathcal{B}_1 \otimes \mathcal{B}_2$ était définie comme tribu engendrée par la partition dont les ensembles sont de la forme $A_1 \times A_2$, où A_1 décrit une partition π_1 engendrant $\mathcal{B}_1$ et A_2 une partition π_2 engendrant $\mathcal{B}_2$. On pose
$$Q(A_1 \times A_2) = P_1(A_1) \times P_2(A_2);$$
Q définit une nouvelle probabilité, qu'on appelle **probabilité produit** et qu'on note $P_1 \otimes P_2$.

II. Applications mesurables

5. 4 INTRODUCTION

Dans la majorité des cas, les éléments des espaces Ω étudiés sont des applications et non des nombres; il arrive cependant fréquemment qu'il suffise de caractériser ces éléments par un nombre réel ou un groupe de nombres réels, c'est-à-dire qu'il suffise de considérer une application X de Ω dans $\mathbb{R}$ ou $\mathbb{R}^d$.

Considérons par exemple le lancement de deux dés non truqués. Cette expérience est naturellement représentée par l'espace Ω des applications de $\{1, 2\}$ dans $\{1, 2, \ldots, 6\}$,

muni de la tribu $\mathcal{T}(\Omega)$ et de la probabilité P uniformément répartie, soit $P(\{\omega\}) = 1/36$ pour tout $\omega \in \Omega$. Si l'on ne s'intéresse qu'à la somme des points indiqués par les dés, il suffit de considérer l'espace $(\tilde{\Omega}, \tilde{\mathcal{B}}; \tilde{P})$, où $\tilde{\Omega} = \{2, 8, \ldots, 12\}$, $\tilde{\mathcal{B}} = \mathcal{T}(\tilde{\Omega})$ et où $\tilde{P}(\{2\}) = \tilde{P}(\{12\}) = 1/36$, $\tilde{P}(\{3\}) = \tilde{P}(\{11\}) = 2/36$, ... Il est clair qu'il y a un moyen de passer de l'un des espaces à l'autre, c'est-à-dire une application X de Ω dans $\tilde{\Omega}$ qui « transporte » la propabilité P de Ω sur $\tilde{\Omega}$ où elle devient $\tilde{P}$.
Pour pouvoir transporter ainsi la probabilité l'application X ne peut être quelconque. Ceci va être formalisé dans les définitions qui suivent.

5. 5 APPLICATIONS MESURABLES. VARIABLES ALÉATOIRES RÉELLES

a) Nous aurons besoin de la notation suivante : si f est une application de Ω_1 dans Ω_2 et B une partie de Ω_2, on notera $f^{-1}(B)$ l'ensemble des éléments $\omega_1 \in \Omega_1$ dont l'image est dans B, soit

$$f^{-1}(B) = \{\omega_1 \in \Omega_1 \mid f(\omega_1) \in B\}.$$

cette notation globale ne suppose pas que f est une bijection. Si f est une bijection, f^{-1} est l'application réciproque habituelle.
Il est facile de vérifier que $f^{-1}(\varnothing) = \varnothing$, $f^{-1}(\Omega_2) = \Omega_1$, $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ $f^{-1}(\complement A) = \complement f^{-1}(A)$, ...

Définition.

Soit $(\Omega_1, \mathcal{B}_1)$ et $(\Omega_2, \mathcal{B}_2)$ deux espaces probabilisables finis. Une application f de Ω_1 dans Ω_2 est dite **mesurable** par rapport à $\mathcal{B}_1$ et $\mathcal{B}_2$ si

$$(\forall A \in \mathcal{B}_2), \quad f^{-1}(A) \in \mathcal{B}_1$$

EXEMPLES

Si $\mathcal{B}_1 = \mathcal{T}(\Omega_1)$ toutes les applications de Ω_1, dans $(\Omega_2, \mathcal{B}_2)$ sont mesurables. Si $\mathcal{B}_1$ est l'algèbre grossière ($\mathcal{B}_1 = \{\varnothing, \Omega_1\}$), les applications mesurables sont les applications constantes; plus généralement si $\mathcal{B}_1$ est engendrée par une partition $(A_1, A_2, \ldots, A_n)$ les applications mesurables sont les applications constantes sur chacun des ensembles de la partition. Inversement, les applications constantes sont mesurables par rapport à tous les espaces de probabilité.

COMPLÉMENT

Soit Ω_1 un ensemble fini et f une application de Ω_1 dans un espace probabilisable fini $(\Omega_2, \mathcal{B}_2)$. La tribu $\mathcal{B}_2$ est engendrée par une partition $(A_1, \ldots, A_n)$; les ensembles $(f^{-1}(A_1))$ forment une partition de Ω_1 qui engendre une tribu $\mathcal{B}_1$ sur Ω_1. L'application f est alors mesurable par rapport à $\mathcal{B}_1$ et $\mathcal{B}_2$.
Si $\mathcal{B}_1'$ est une autre tribu sur Ω_1 telle que f soit mesurable par rapport à $\mathcal{B}_1'$ et $\mathcal{B}_2$, alors $\mathcal{B}_1' \supset \mathcal{B}_1$. On dit que $\mathcal{B}_1$ est la plus petite tribu rendant f mesurable, ou encore est la tribu **engendrée par** f sur Ω_1.
Cherchez quelle est la tribu engendrée par l'application X du paragraphe précédent.

b) Soit maintenant X une application de $(\Omega, \mathcal{B})$ dans $\mathbb{R}^d$. L'image $X(\Omega)$ de Ω par X est un ensemble fini; on peut le munir de la tribu $\mathcal{T}(X(\Omega))$ et l'on pose :

Définition.

Une application X de $(\Omega, \mathcal{B})$ dans $\mathbb{R}^d$ sera appelée **variable aléatoire vectorielle** si elle est mesurable par rapport à $\mathcal{B}$ et à $\mathcal{T}(X(\Omega))$. Si $d = 1$, on dira que X est une **variable aléatoire réelle** et on écrira en abrégé v.a.r.

Remarque : Cette dénomination n'est pas très heureuse, car d'une part X n'est pas une variable mais une application, qui a tout $\omega \in \Omega$ fait correspondre un nombre $X(\omega)$ bien déterminé. La bonne expression est celle d'application mesurable. Nous emploierons néanmoins l'expression de variable aléatoire, d'une part pour se conformer à un usage universel, d'autre part par ce que ce terme spécifie que l'espace d'arrivée de l'application considérée est un sous-ensemble fini de $\mathbb{R}^d$ et non pas un espace probabilisable arbitraire.

Théorème.

L'application X de $(\Omega, \mathfrak{B})$ dans $\mathbb{R}^d$ est une variable aléatoire vectorielle si et seulement si pour tout $x \in \mathbb{R}^d$,

$$\{\omega : X(\omega) = x\} \in \mathfrak{B}.$$

Démonstration. Si X est une variable aléatoire et si $x \in X(\Omega)$ alors $\{\omega : X(\omega) = x\} \in \mathfrak{B}$ d'après la définition précédente. Si $x \notin X(\Omega)$ alors $\{\omega : X(\omega) = x\} = \varnothing \in \mathfrak{B}$.
Réciproquement, Ω étant finie, si $A \in \mathfrak{P}(X(\Omega))$ il existe un nombre fini n d'éléments x_i de $\mathbb{R}^d$ tels que $A = \{x_1, \ldots, x_n\}$ et

$$X^{-1}(A) = \bigcup_{i=1}^{n} \{\omega : X(\omega) = x_i\};$$

chacun des ensembles de cette réunion étant dans $\mathfrak{B}$ par hypothèse, $X^{-1}(A)$ est aussi dans $\mathfrak{B}$ et X est une variable aléatoire.

REMARQUE

Cette proposition ne s'étend pas aux espaces probabilisables quelconques. Elle exige que l'espace Ω soit fini.

Théorème.

L'application X de $(\Omega, \mathfrak{B})$ dans $\mathbb{R}$ est une v.a.r., si et seulement si

$$(\forall x \in R) \qquad \{\omega : X(\omega) < x\} \in \mathfrak{B}.$$

Démonstration. Soient $x_1 < x_2 < \ldots < x_p$ les éléments de $X(\Omega)$ rangés par ordre croissant.
Si X est une v.a.r. et si n est le rang du plus grand élément de $X(\Omega)$ inférieur à x, on a

$$\{\omega : X(\omega) < x\} = \bigcup_{i=1}^{n} \{\omega : X(\omega) = x_i\},$$

et cet ensemble est dans $\mathfrak{B}$.
Réciproquement, soit X telle que $\{\omega : X(\omega) < x\} \in \mathfrak{B}$ pour tout $x \in \mathbb{R}$; pour $x_n \in X(\Omega)$ il existe deux nombres réels x et x' tels que $x_{n-1} < x < x_n < x' < x_{n+1}$, et l'on a

$$\{\omega : X(\omega) = x_n\} = \{\omega : X(\omega) < x'\} - \{\omega : X(\omega) < x\} \in \mathfrak{B},$$

ce qui prouve que X est une v.a.r.

Théorème.

L'ensemble des v.a.r. définies par un espace $(\Omega, \mathfrak{B})$ peut être muni d'une structure d'espace vectoriel sur le corps des réels.

Démonstration. Si X est une v.a.r. et α un nombre réel on définit une nouvelle application (αX) de Ω dans $\mathbb{R}$ en posant

$$(\alpha X)(\omega) = \alpha X(\omega);$$

on a alors, si $\alpha \neq 0$, $\{\omega : (\alpha X)(\omega) = x\} = \{\omega : X(\omega) = x/\alpha\} \in \mathcal{B}$, et si $\alpha = 0$, $\{\omega (\alpha X)(\omega) = x\} = \varnothing$ ou Ω suivant que $x = 0$ ou que $x \neq 0$; (αX) est donc encore une v.a.r.

Si X et Y sont deux v.a.r., on définit l'application $X + Y$ de Ω dans $\mathbb{R}$ par

$$(X + Y)(\omega) = X(\omega) + Y(\omega).$$

Supposons que $X(\Omega) = \{x_1, x_2, \ldots, x_p\}$, $Y(\Omega) = \{y_1, y_2, \ldots, y_q\}$ alors $(X + Y)(\Omega)$ est l'ensemble des nombres $x_i + y_j$ avec $x_i \in X(\Omega)$ et $y_j \in Y(\Omega)$ et l'on a

$$\{\omega : (X + Y)(\omega) = x\} = \bigcup_{i,j} \{\omega : X(\omega) = x_i, Y(\omega) = y_j\}$$

où la réunion est étendue à tous les couples i, j tels que $x_i + y_j = x$. Cette réunion étant une réunion finie, est encore un ensemble de $\mathcal{B}$ et $X + Y$ est une v.a.r.

Vous vérifierez facilement que pour ces deux opérations l'ensemble des v.a.r. définies sur $(\Omega, \mathcal{B})$ est un espace vectoriel.

Définition.

αX s'appelle le **produit de X par le scalaire** α et $X + Y$ la **somme** de X et Y.

La somme d'un nombre fini de v.a.r. et toute combinaison linéaire de v.a.r. est encore une v.a.r.

De même le produit XY de deux v.a.r. est encore une v.a.r. Soit en effet a un nombre réel et I l'ensemble des couples (i, j) tels que $x_i y_j = a$. L'ensemble I est évidemment de cardinal fini et l'on a

$$\{\omega : X(\omega)\, Y(\omega) = a\} = \bigcup_{(i,j) \in I} \{\omega : X(\omega) = x_i, Y(\omega) = y_j\};$$

cet ensemble est donc encore un ensemble de $\mathcal{B}$.

EXERCICES

1. Si X et Y sont deux v.a.r. définies sur $(\Omega, \mathcal{B})$ montrer que l'application $X \wedge Y$ qui à $\omega \in \Omega$ fait correspondre le plus petit des deux nombres $X(\omega)$ et $Y(\omega)$ est encore une v.a.r. Cherchez à exprimer $\{\omega : (X \wedge Y)(\omega) < x\}$ en fonction de $\{\omega : X(\omega) < x\}$ et $\{\omega : Y(\omega) < x\}$.
2. Si f est une application de $\mathbb{R}$ dans $\mathbb{R}$ et si X est une v.a.r. alors l'application $f \circ X$ de Ω dans $\mathbb{R}$ est aussi une v.a.r.

5. 6 SYSTÈMES DE VARIABLES ALÉATOIRES

Soit X une variable aléatoire vectorielle à valeur dans $\mathbb{R}^d$ et $\{e_1, \ldots, e_d\}$ la base canonique de $\mathbb{R}^d$ ($e_1 = (1, 0, \ldots, 0)$, $e_2 = (0, 1, \ldots)$ ... .). On peut écrire de manière unique

$$X(\omega) = X^1(\omega)\, e_1 + \ldots + X^d(\omega)\, e_d.$$

Pour tout i $(1 \leqslant i \leqslant d)$, X^i est une application de Ω dans $\mathbb{R}$ et pour $x \in \mathbb{R}$,

$$\{\omega : X^i(\omega) = x\} = \{\omega : X(\omega) = (x^1 e_1 + \ldots + x e_i + \ldots + x^n e_n)\}$$

où les nombres $x^1, \ldots x^{i-1}, x^{i+1}, \ldots x^n$ sont arbitraires. Cette réunion étant une réunion finie d'ensembles de $\mathcal{B}$, est encore un ensemble de $\mathcal{B}$. L application X^i est donc encore une v.a.r.

Réciproquement si on se donne d variables aléatoires réelles X^i définies sur le même espace $(\Omega, \mathcal{B})$, en posant

$$X(\omega) = X^1(\omega)\, e_1 + \ldots + X^d(\omega)\, e_d,$$

on définit une variable aléatoire vectorielle à valeur dans $\mathbb{R}^d$.

Définition.

On appelle encore **système de d variables aléatoires réelles** un ensemble de d v.a.r. définies sur le même espace $(\Omega, \mathcal{B})$. Si $d = 2$, on dit que l'on a un **couple de v.a.r.**

Nous venons de voir que la donnée d'un système de d v.a.r. est équivalente à la donnée d'une variable vectorielle.

EXEMPLE

On tire au hasard un individu dans une population Ω finie donnée et l'on note son poids et sa taille, on obtient ainsi un couple de v.a.r. défini sur $(\Omega, \mathcal{T}(\Omega))$.

5. 7 PROBABILITÉS IMAGES

Voyons maintenant comment on peut transporter les probabilités au moyen des applications mesurables. Soit $(\Omega_1, \mathcal{B}_1, P)$ un espace de probabilité, $(\Omega_2, \mathcal{B}_2)$ un espace probabilisable et f une application mesurable par rapport à $\mathcal{B}_1$ et $\mathcal{B}_2$. On définit une application Q de $\mathcal{B}_2$ dans $[0, 1]$ en posant pour $A \in \mathcal{B}_2$,

$$Q(A) = P(f^{-1}(A)).$$

Ceci a toujours un sens, puisque f étant mesurable, $f^{-1}(A) \in \mathcal{B}_1$; c'est justement pour cela qu'on a ainsi défini les applications mesurables.
Vérifions que Q est une probabilité sur $(\Omega_2, \mathcal{B}_2)$. D'une part

$$Q(\Omega_2) = P(f^{-1}(\Omega_2)) = P(\Omega_1) = 1;$$

d'autre part si A et B sont deux éléments disjoints de $\mathcal{B}_2$, $f^{-1}(A)$ et $f^{-1}(B)$ sont également disjoints dans Ω_1 et l'on a

$$\begin{aligned} Q(A \cup B) &= P(f^{-1}(A \cup B)) = P(f^{-1}(A) \cup f^{-1}(B)) \\ &= P(f^{-1}(A)) + P(f^{-1}(B)) = Q(A) + Q(B). \end{aligned}$$

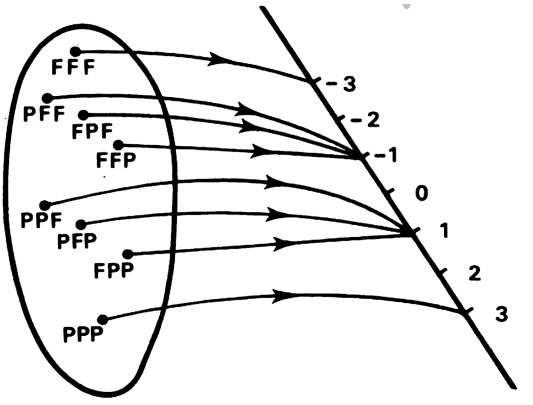
Définition.

La probabilité Q s'appelle **probabilité image** de P par f.

EXEMPLES

1. Dans l'exemple de l'introduction la probabilité $\tilde{P}$ est l'image de P par X qui à une application ω de $\{1, 2\}$ dans $\{1, 2, \ldots, 6\}$ fait correspondre la somme des nombres images.
2. De façon générale si X est une v.a.r. définie sur $(\Omega, \mathcal{B}, P)$, la probabilité image de P par X est une probabilité sur $(X(\Omega), \mathcal{T}(X(\Omega)))$. Soit par exemple un joueur qui joue trois fois de suite à pile ou face avec une pièce non truquée. Un modèle de cette expérience est fourni par l'espace $\Omega = \{PPP, PPF, PFP, \ldots\}$ muni de la tribu $\mathcal{T}(\Omega)$ et de la probabilité uniformément répartie. Supposons que ce joueur gagne 1 franc si pile sort et perd 1 franc si face sort et que nous nous intéressions seulement à l'état de ses finances à la fin du jeu, sans vouloir tenir compte de l'ordre des pertes et des gains. Nous nous intéresserons donc à la variable aléatoire décrite dans le diagramme ci-dessous (fig. 2).

fig. 2



On a $X(\Omega) = \{-3, -1, 1, 3\}$ et la probabilité image de P par X est donnée de manière évidente par

$$Q(-3) = 1/8, \quad Q(-1) = 3/8, \quad Q(1) = 3/8, \quad Q(3) = 1/8.$$

EXERCICES

1. Généraliser la description précédente à 4 puis à n lancers successifs; quelle est la probabilité d'avoir p faces dans une suite de n lancers? Cette question revient à trouver la probabilité image de la probabilité uniformément répartie sur l'ensemble de tous les lancers possibles par une application qui généralise l'application X précédente.

Nous avons vu dans le paragraphe 5 qu'une application X de $(\Omega, \mathcal{B})$ dans $\mathbb{R}$ était une v.a.r. si et seulement si pour tout x de $\mathbb{R}$ on a

$$\{\omega : X(\omega) < x\} \in \mathcal{B}.$$

Si X est définie sur un espace de probabilité $\{\Omega, \mathcal{B}, P\}$ l'expression

$$P(\{\omega : X(\omega) < x\})$$

a donc un sens; on l'écrira plus simplement $P(X < x)$.

Définition.

Si X est une v.a.r. définie sur l'espace de probabilité $(\Omega, \mathcal{B}, P)$ on appelle **fonction de répartition** de X l'application

$$x \longrightarrow F(x) = P(X < x)$$

de $\mathbb{R}$ dans $[0, 1]$.

La probabilité image de P par X s'appelle la **loi de probabilité** de X; on la désigne aussi quelquefois comme la **répartition** de X.

Des propriétés de la probabilité P on déduit celles de la fonction de répartition.

Soient $x_1 < x_2 \ldots < x_n$ les éléments de $X(\Omega)$ rangés par ordre croissant. Si $x < x_1$, on a $\{\omega : X(\omega) < x\} = \varnothing$ et donc $F(x) = P(\varnothing) = 0$; si $x < x_n$ on a de même $F(x) = 1$. Si $x < x'$, $\{\omega : X(\omega) < x\}$ et $\{\omega : x < X(\omega) < x'\}$ sont deux ensembles disjoints dans $\mathcal{B}$ et l'on a donc

$$F(x') = F(x) + P(\{\omega : x < X(\omega) < x'\}).$$

Il en résulte que $F(x') > F(x)$, autrement dit F est croissante.

D'autre part s'il existe $x_i \in X(\Omega)$ tel que $x_i < x < x' \leqslant x_{i+1}$ on a $\{\omega : x < X(\omega) < x'\} = \varnothing$ et par suite $F(x) = F(x')$; F est donc constante sur les intervalles $]x_i \ , \ x_{i+1}]$.

Inversement, $\{\omega : x_i \leqslant X(\omega) < x_{i+1}\} = \{\omega : X(\omega) = x_i\}$ et l'on a

$$P(\{\omega : X(\omega) = x_i\}) = F(x_{i+1}) - F(x_i).$$

La fonction de répartition donne un moyen de calculer la probabilité image de P par X.

EXEMPLES

1. La fonction de répartition de la variable X définie plus haut sur l'espace de trois lancers successifs d'une même pièce a le graphe ci-dessous (fig. 3).

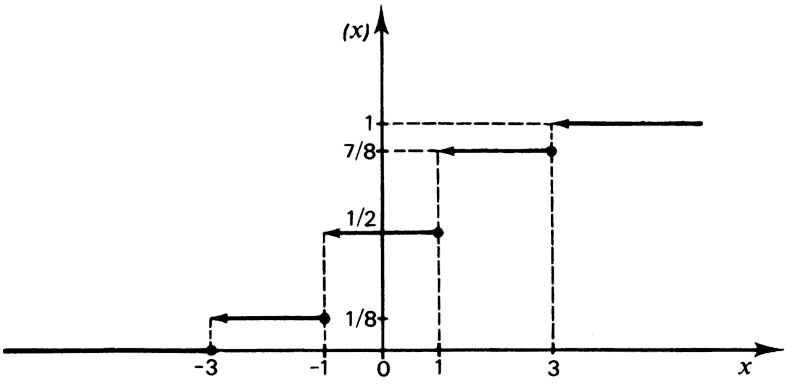


fig. 3

2. ATTENTION ! Deux v.a.r. différentes, peuvent avoir la même fonction de répartition et donc la même loi de probabilité. Soit par exemple le lancer d'une pièce non truquée : constatez que la v.a.r. X qui prend la valeur 1 pour pile et -1 pour face et la v.a.r. Y qui prend la valeur -1 pour pile et 1 pour face ont même fonction de répartition.

EXERCICES

2. Soit X une v.a.r. définie sur un espace $(\Omega, \mathfrak{B}, P)$ et dont la fonction de répartition F est donnée par

$$\begin{array}{lll} F(x) = 0 & \text{pour} & x \leqslant -1, \\ F(x) = 1/2 & \text{pour} & -1 < x \leqslant 1, \\ F(x) = 3/4 & \text{pour} & 1 < x \leqslant 2, \\ F(x) = 1 & \text{pour} & 2 < x. \end{array}$$

Déterminer $X(\Omega)$ et la probabilité image de P par X.

3. Soit X une v.a.r.; étudier les propriétés de la fonction

$$G(x) = P(X \leqslant x);$$

en quoi diffère-t-elle de $F(x)$?

Dans le cas des variables aléatoires vectorielles les probabilités images ont des noms traditionnels que nous allons donner maintenant.

Définition.

Si $(X^1, \ldots, X^d)$ est un système de n v.a.r. définies sur un espace $(\Omega, \mathfrak{B}, P)$ on appelle **loi conjointe** de ce système la probabilité image de P par l'application

$$X(\omega) = X^1(\omega)\, e_1 + X^2(\omega)\, e_2 + \ldots + X^d(\omega)\, e_d$$

de Ω de $\mathbb{R}^d$. On appelle **lois marginales** les probabilités images de P par chacune des applications X^i.

Se donner la loi conjointe d'un système $(X^1, \ldots, X^d)$ est équivalent à se donner tous les nombres

$$P(X^1 = x_1, X^2 = x_2, \ldots, X^d = x_d)$$

où $(x_1, \ldots, x_d)$ décrit $X(\Omega)$.
Considérons l'espace de probabilité $(X(\Omega), \mathfrak{T}(X(\Omega)), Q)$ où Q est la loi conjointe du système $(X^1, \ldots, X^d)$. Soit C_i l'application qui à un point de $X(\Omega)$ fait correspondre sa $i^{\text{ème}}$ coordonnée :

$$(x_1, \ldots, x_d) \longrightarrow x_i.$$

L'application C_i est mesurable de $(X(\Omega), \mathfrak{T}(X(\Omega)))$ dans $(X^2(\Omega), \mathfrak{T}(X^2(\Omega)))$ et si $y \in X^2(\Omega)$ on a

$$\begin{aligned} Q(C_i^{-1}\{y\}) &= Q(\{x_1, \ldots, x_d\} \in X(\Omega) \mid y = x_i\}) \\ &= P(\{\omega : X^i(\omega) = y\}) \end{aligned}$$

par définition de Q. On a ainsi démontré :

Théorème.

Les lois marginales sont les probabilités images de la loi conjointe par les applications coordonnées C_i.

Dans le cas d'un couple de v.a.r. on peut donner une représentation graphique de la loi conjointe et des lois marginales. Soit $X = X^1 e_1 + X^1 e_2$ une variable aléatoire à valeur dans $\mathbb{R}^2$, et supposons que

$$X^1(\Omega) = (x_1^1, x_2^1, \ldots, x_i^1, \ldots x_p^1) \quad \text{et} \quad X^2(\Omega) = (x_1^2, \ldots, x_j^2, \ldots, x_q^2),$$

alors $X(\Omega) = \{(x_i^1, x_j^2);\ 1 < i < p,\ 1 < j < q\}$. La loi conjointe de X^1 et X^2 est donnée par les nombres

$$p_{ij} = P(\{\omega : X(\omega) = (x_i^1, x_j^2)\}),$$

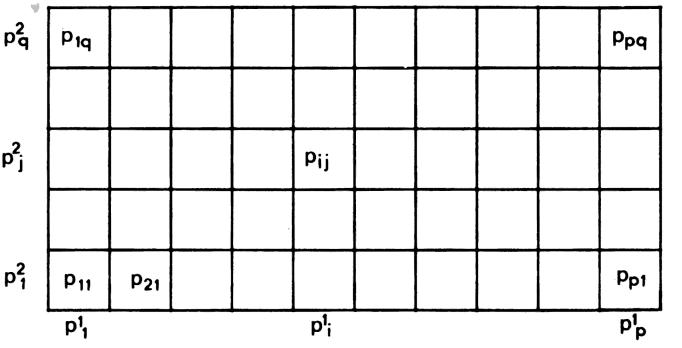
et les lois marginales par les nombres

$$\begin{aligned} p_i^1 &= P(\{\omega : X^1(\omega) = x_i^1\}), \\ p_j^2 &= P(\{\omega : X^2(\omega) = x_{jj}^2\}). \end{aligned}$$

D'après la proposition précédente on a

$$p_i^1 = \sum_{j=1}^{q} p_{ij}, \qquad p_j^2 = \sum_{i=1}^{p} p_{ij}.$$

fig. 4



On peut représenter ceci au moyen d'un tableau rectangulaire (fig. 4) où l'on trouve p_{ij} à l'intersection de la $i^{\text{ème}}$ colonne et de la $j^{\text{ème}}$ ligne.

On a évidemment

$$\sum_{i\times j} p_{ij} = \sum_{i=1}^{p} p_i^1 = \sum_{j=1}^{q} p_j^2 = 1.$$

ATTENTION ! Les mêmes lois marginales peuvent correspondre à des lois conjointes différentes, comme le prouve les deux exemples suivants (fig. 5).

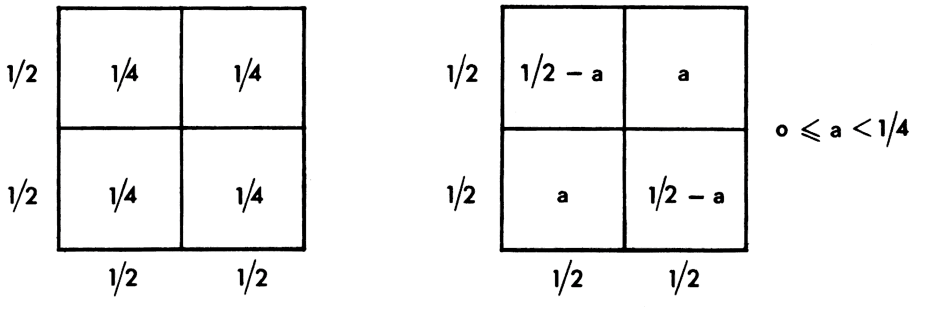


fig. 5

EXERCICE

3. On jette deux dés non truqués et on considère les v.a.r. égales au plus petit des deux nombres indiqués soit X^1 et au plus grand des deux nombres indiqués soit X^2. Dresser le tableau donnant la loi conjointe et les lois marginales.

III. Indépendance

5. 8 INTRODUCTION

Considérons l'espace de probabilité suivant correspondant au tirage au hasard d'une carte dans un jeu de 32 : Ω est l'ensemble des cartes dessiné ci-dessous (fig. 6),

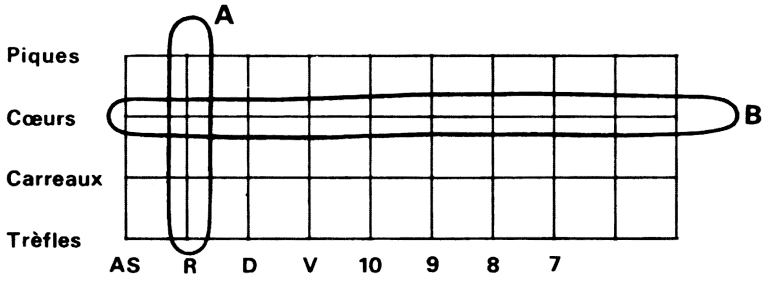


fig. 6

$\mathfrak{B} = \mathfrak{T}(\Omega)$ et P est la probabilité uniformément répartie. Considérons les deux événements : A = {ensemble des rois} et B = {ensemble des cœurs}, supposez que quelqu'un tire une carte et vous dise que c'est un cœur sans préciser lequel, autrement dit vous savez que B est réalisé mais vous ne savez pas sur lequel des éléments de B on est tombé; pouvez-vous dire quelque chose de plus qu'auparavant quant à la réalisation de l'événement A? La découverte du point exact de B sur lequel on est tombé peut être assimilé à une deuxième expérience aléatoire où cette fois on aura $\Omega' = B$, $\mathfrak{B}' = \mathfrak{T}(B)$ et où P' sera uniformément répartie sur B. La probabilité de tirer le roi de cœur dans cette deuxième expérience est 1/8 et c'est la seule façon pour que A soit aussi réalisé. Or la probabilité initiale de A, c'est-à-dire la probabilité de tirer un roi était aussi 1/8. Autrement dit le fait de savoir que B était réalisé n'a pas « changé » la probabilité de A. On dit que A et B sont indépendants et l'on constate que

$$P(A \cap B) = P(A)\,P(B).$$

Pensez maintenant au jet de deux dés. Les v.a.r. X^1 et X^2 égales aux nombres indiqués sont intuitivement « indépendantes ». Le fait de connaître la valeur prise par l'une des deux n'apporte aucune information supplémentaire sur la valeur prise par l'autre. Si l'on prend pour modèle ce jet, l'espace de probabilité déjà décrit où la probabilité est uniformément répartie sur l'ensemble des cas possibles, il est facile de calculer que pour $A_1, A_2 \subset \{1, 2, \ldots, 6\}$ on a

$$P(\{\omega . X^1(\omega) \in A_1\} \cap \{\omega : X^2(\omega) \in A_2\}) = P(\{\omega : X^1(\omega) \in A_1\})\,P(\{\omega : X^2(\omega) \in A_2\}).$$

Nous allons formaliser ceci dans les définitions qui vont suivre.

5. 9 SYSTÈMES DE VARIABLES INDÉPENDANTES

Définition.

Des v.a.r. $(X^1, X^2, \ldots, X^n)$ définies sur un même espace de probabilité $(\Omega, \mathfrak{B}, P)$ sont dites **indépendantes** si quels que soient les ensembles $A_i \subset X^i(\Omega)$, $(i = 1, 2, \ldots n)$, on a

$$P\left(\bigcap_{i=1}^{n} \{\omega : X^i(\omega) \in A_i\}\right) = \prod_{i=1}^{n} P(\{\omega : X^i(\omega) \in A_i\}).$$

On rappelle que $\prod_{i=1}^{n} P(\{\omega : X(\omega) \in A_i\})$ est le produit des nombres $P(\{\omega : X^i(\omega) \in A_i\})$.

Il suffit que ces relations soient vérifiées pour les ensembles A_i réduits à un point.

Soit $A \in \mathfrak{B}$; on peut lui associer l'application φ_A à valeurs dans R définie par

$$\varphi_A(\omega) = 1 \text{ si } \omega \in A, \quad \varphi_A(\omega) = 0 \text{ si } \omega \notin A.$$

On a $\{\omega : \varphi_A(\omega) = 1\} = A$ et $\{\omega : \varphi_A(\omega) = 0\} = \complement A$ et donc φ_A est une v.a.r.

Définition.

On dit que des événements $A_1, \ldots, A_n \in \mathfrak{B}$ sont **indépendants** si les v.a.r. φ_{A_i} sont indépendantes.

Il est équivalent de dire que l'on a

$$(1) \qquad P\left(\bigcap_{i=1}^{n} B_i\right) = \prod_{i=1}^{n} P(B_i) = P(B_1) \ldots P(B_n)$$

quelle que soit la façon dont on choisit B_i dans l'ensemble $\{\Omega, \varnothing, A_i, \complement A_i\}$.

REMARQUE

La probabilité P joue un rôle essentiel dans cette définition. Si on changeait la probabilité sur $(\Omega, \mathfrak{B})$ des variables qui étaient indépendantes pourraient ne plus l'être.

Dans le cas d'un couple d'événements ou de variables les formulations de la notion d'indépendance peuvent être simplifiées. Ainsi pour que deux événements A et B soient indépendants il suffit que

$$P(A \cap B) = P(A)\,P(B).$$

On peut en effet montrer toutes les autres relations (1) à partir de celle-ci. On a par exemple :

$$\begin{aligned} P(\complement A \cap \complement B) = 1 - P(A \cup B) &= 1 - P(A) - P(B) + P(A \cap B) \\ &= 1 - P(A) - P\,B) + P(A)\,P(B) \\ &= (1 - P(A))\,(1 - P(B)). \end{aligned}$$

Soient maintenant X^1 et X^2 deux variables aléatoires indépendantes. Si $X = X^1 e_1 + X^2 e_2$, on a, avec les notations du paragraphe précédent,

$$\begin{aligned} p_{ij} &= P(\{\omega : X(\omega) = (x_i^1, x_j^2)\}) \\ &= P(\{\omega : X^1(\omega) = x_i^1\} \cap \{\omega : X^2(\omega) = y_j^2\}) \\ &= P(\{\omega : X^1(\omega) = x_i^1\}) \times P(\{\omega : X^2(\omega) = x_j^2\}) = p_i^1 \times p_j^2. \end{aligned}$$

On énoncera ceci en disant que la loi conjointe de X^1 et X^2 est le **produit** des lois marginales. Réciproquement si la loi conjointe de deux v.a.r. X^1 et X^2 est telle que $\forall\, i, j$ on ait $p_{ij} = p_i^1 \times p_j^2$, ces v.a.r. sont indépendantes.

Théorème.

Deux v.a.r. définies sur le même espace $(\Omega, \mathfrak{B}, P)$ sont indépendantes si et seulement si leur loi conjointe est le produit de leurs lois marginales.

EXEMPLE

De deux couples de v.a.r. dont les lois seraient données par la figure 5, le premier serait constitué de v.a.r. indépendantes et non le second.
Pour des lois marginales données il existe une seule loi conjointe correspondant à un couple de v.a.r. indépendantes.

On peut aussi énoncer la notion d'indépendance au moyen des fonctions de répartition.

Théorème.

Des v.a.r. $(X^1, \ldots, X^n)$ définies sur le même espace $(\Omega, \mathfrak{B}, P)$ sont indépendantes si et seulement si, quels que soient les nombres réels $x_1, \ldots, x_n$ on a

$$P\{\omega : X^1(\omega) < x_1, X^2(\omega) < x_2, \ldots, X^n(\omega) < x_n\}) = \prod_1^n F^i(x_i)$$

où F^i est la fonction de répartition de X^i.

Démonstration : Pour chaque variable X^i, soit A_i l'ensemble des nombres de $X^i(\Omega)$ inférieur à x_i; on a alors $P(A_i) = F^i(x_i)$ par définition de F^i et

$$P(\{\omega : X^1(\omega) < x_1, X^2(\omega) < x_2, \ldots, X^n(\omega) < x_n\})$$
$$= P(\{\omega : X^1(\omega) \in A_1, X^2(\omega) \in A_2, \ldots, X^n(\omega) \in A_n\}) = \prod_1^n F^i(x_i),$$

puisque le X^i sont indépendantes.

Réciproquement soit $a_i \in X^i(\Omega)$ et x_i et x_i' deux nombres réels tels que a_i soit le seul élément de $X^i(\Omega)$ compris entre x_i et x_i' $(x_i < a_i < x_i')$. On a

$$P(X^i = a_i) = F^i(x_i) - F^i(x_i').$$

On a d'autre part, pour des réels arbitraires y_i,

$$P(X^1 = a_1, X^2 < y_2, \ldots, X^n < y_n) =$$
$$P(X^1 < x_1', X^2 < y_2, \ldots, X^n < y_n) - P(X^1 < x_1, X^2 < y_2, \ldots, X^n < y_n) =$$
$$F^1(x_1') \cdot \prod_{i=2}^n F^i(y_i) - F^1(x_1) \cdot \prod_{i=2}^n F^i(x_i') = P(X^1 = a_1) \cdot \prod_{i=2}^n F^i(y_i').$$

Nous pouvons maintenant recommencer ceci avec X^2 et écrire

$$P(X^1 = a_1, X^2 = a_2, X^3 < y_3, \ldots) =$$
$$P(X^1 = a_1, X^2 < x_2', \ldots) - P(X^1 = a_1, X^2 < x^2, \ldots) =$$
$$P(X^1 = a_1)\, P(X^2 = a_2) \cdot \prod_{i=3}^n F^i(y_i).$$

De proche en proche on montre ainsi que

$$P(X^1 = a_1, X^2 = a^2, \ldots, X^n = a_n) = \prod_{i=1}^n P(X^i = a_i)$$

et donc que les v.a.r. X^i sont indépendantes.

COMPLÉMENTS

On dit que les tribus $\mathfrak{B}_i$ $(i = 1, 2, \ldots, n)$ contenues dans le tribu $\mathfrak{B}$ d'un espace $(\Omega, \mathfrak{B}, P)$ sont **indépendantes** si pour tout choix de $B_i \in \mathfrak{B}_i$ on a

$$P(B_1 \cap B_2 \ldots \cap B_n) = \prod_{i=1}^n P(B_i).$$

Dire que des v.a.r. sont indépendantes c'est-à-dire que les tribus qu'elles engendrent sont indépendantes. Inversement si des tribus sont indépendantes, des v.a.r. X arbitraires mais mesurables par rapport aux $\mathcal{B}_i$ sont indépendantes. Nous retrouvons ici comme cas particulier le fait que la définition de l'indépendance des ensembles fait intervenir de façon symétrique les ensembles et leurs complémentaires. Considérons maintenant l'espace de probabilité produit définie au § II.2. Parmi les tribus contenues dans $\mathcal{B}_1 \otimes \mathcal{B}_2$, il y a la tribu $\widetilde{\mathcal{B}}_1$ des ensembles de la forme $A_1 \times \Omega_2$ avec $A_1 \in \mathcal{B}_1$ et la tribu $\widetilde{\mathcal{B}}_2$ des ensembles de la forme $\Omega_1 \times A_2$ avec $A_2 \in \mathcal{B}_2$. La probabilité produit $P_1 \otimes P_2$ rend ces deux tribus indépendantes.

5. 10 LOIS BINOMIALES. ÉPREUVES RÉPÉTÉES

Supposons que nous disposions d'une urne dans laquelle sont placées a boules rouges et b boules bleues indiscernables au toucher. Nous en tirons une au hasard, puis après avoir noté sa couleur nous la remélangeons avec les autres. Si nous faisons un 2e tirage, il y a tout lieu de penser que la couleur de la boule tirée ne dépend en aucune manière de la couleur de la première boule. On peut ainsi faire n tirages au cours desquels on peut tirer de 0 à n boules rouges. Quelle est la probabilité d'obtenir ainsi k boules rouges? Au $i^{\text{ème}}$ tirage nous pouvons associer une application X^i qui prendra la valeur 1 si la boule tirée est rouge et 0 sinon. Soit $Y^n = X^1 + X^2 + \ldots + X^n$; la question posée est équivalente à la suivante : quelle est la probabiéité que Y^n prenne la valeur k.
Formalisons ceci mathématiquement. Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité tel qu'on puisse définir dessus n v.a.r. X^i indépendantes et telles que pour tout i

$$P(\{X^i = 1\}) = p, \quad P(\{X^i = 0\}) = q$$

avec $p + q = 1$ (dans l'exemple précédent on aurait $p = a/a + b$, $q = b/a + b$). Posons $Y^n = X^1 + \ldots + X^n$; Y^n est une v.a.r. puisqu'une somme de v.a.r. est encore une v.a.r. Considérons les événements

$$\{X^1 = S_1, \quad X^2 = S_2, \quad \ldots, \quad X^n = S_n\}$$

où $S_1, \ldots, S_n$ sont égaux à 0 ou à 1 et tels que $S_1 + S_2 + \ldots + S_n = k$. Un de ces événements est complètement déterminé lorsqu'on a choisi le rang de S_i égaux à 1 et ceci peut se faire de C_n^k façons différentes. Si deux suites de nombres S_i sont différentes, les événements correspondants sont disjoints puisqu'ils sont contenus dans les événements disjoints $\{X^i = 0\}$ et $\{X^i = 1\}$ pour une variable X^i au moins. Enfin d'après l'hypothèse d'indépendance on a

$$P(X^1 = S_1, X^2 = S_2, \ldots, X^n = S_n) = p^k q^{n-k}.$$

Comme l'événement $Y^n = k$ est la réunion de ces événements, on a

$$P(\{\omega : Y^n(\omega) = k\}) = C_n^k p^k q^{n-k}.$$

L'entier k ne peut prendre que les valeurs 0, 1, ..., n et l'on vérifie bien grâce à la formule du binôme que

$$\sum_{p=0}^{n} C_n^k p^k q^{n-k} = (p + q)^n = 1.$$

C'est pourquoi la probabilité image de Y^n s'appelle **loi binomiale.** On dit aussi que Y^n est une variable aléatoire binomiale.

EXERCICES

1. Calculer, dans l'exemple initial, la probabilité de tirer 3 boules rouges en 5 tirages, si $a = 2$ et $b = 4$.
2. Pour $p = q = 1/2$, tracer les fonctions de répartitions de Y^n pour $n = 1, 2, 3, 4, 5, \ldots$.

REMARQUE

On peut toujours construire un espace $(\Omega, \mathfrak{B}, P)$ sur lequel on peut définir des v.a.r. X^i ayant les propriétés que nous venons d'étudier. On prend pour espace Ω l'ensemble des suites de n symboles S ou E (ou ce qui est équivalent l'ensemble des applications de $\{1, 2, \ldots, n\}$ dans $\{S, E\}$), $\mathfrak{B} = \mathfrak{T}(\Omega)$, et $P(\{\omega\}) = p^k q^{n-k}$ si ω contient k fois le symbole S. Les variables X^i égales à 1 sur les $\omega \in \Omega$ qui ont un S à la $i^{ème}$ place et à 0 sinon répondent aux conditions ci-dessus.

IV. Espérance mathématique. Variance

5.11 ESPÉRANCE MATHÉMATIQUE

Soit X une v.a.r. définie sur une espace $(\Omega, \mathfrak{B}, P)$, x_i $(i = 1, 2, \ldots, n)$ les éléments de $X(\Omega)$; on définit la probabilité image de P par X par les nombres

$$p_i = P(X = x_i).$$

Définition.

On appelle espérance mathématique ou moyenne de la v.a.r. X le nombre

$$E(X) = \sum_{i=1}^{n} p_i x_i.$$

Comme $\sum_{i=1}^{n} p_i = 1$, on voit que E(X) est le barycentre des points x_i affectés des coefficients p_i. Ce nombre indique une « valeur moyenne » pour la v.a.r. X ce qui va apparaître plus clairement dans les exemples et dans certains théorèmes qui vont suivre. Si $E(X) = 0$, la v.a.r. X est dite **centrée.** Par exemple la v.a.r. qui prend la valeur 1 avec la probabilité 1/2 et la valeur -1 avec la probabilité 1/2 est centrée. Pour toute v.a.r. X, la nouvelle v.a.r. $X - E(X)$, obtenue en retranchant de X la v.a.r. constante E(X), est centrée.

EXEMPLES

1. Si X prend la valeur 1 avec la probabilité p et la valeur 0 avec la probabilité $1 - p$, on a

$$E(X) = p.$$

En particulier, si X est la v.a.r. φ_A associée à l'élément A qui a été définie au paragraphe III.2 on a

$$E(\varphi_A) = P(A).$$

L'espérance mathématique apparaît ainsi comme un prolongement de la probabilité, des ensembles aux fonctions mesurables.

2. Quelle est l'espérance mathématique de la v.a.r. binomiale Y^n définie au paragraphe précédent? On a

$$E(Y^n) = \sum_{k=0}^{n} kC_n^k q^{n-k}$$

$$= \sum_{k=1}^{n} k \frac{n!}{k!(n-k)!} p^k q^{n-k}$$

$$= np \sum_{k=1}^{n} \frac{(n-1)!}{(k-n)!(n-k)!} p^{k-1} q^{n-k},$$

et en changeant k en $k-1$,

$$E(Y^n) = np \left(\sum_{k=0}^{n} \frac{(n-1)!}{k!(n-1-k)!} p^{k-1} q^{n-1-k} \right);$$

on reconnaît là le développement du binôme pour $(p+q)^{n-1}$, on a donc

$$E(Y^n) = np(p+q)^{n-1} = np$$

puisque $p + q = 1$. On remarque que ce résultat est conforme à l'intuition : si on fait de nombreux tirages indépendants dans une population contenant deux espèces en proportions p et q, le « nombre moyen » d'individus d'une espèce à avoir été tiré doit être proportionnel à p et au nombre de tirages. Ceci sera précisé ultérieurement.
La variable centrée correspondant à Y^n est $Y^n - np$.

Soit maintenant (X^1, X^2) un couple de v.a.r. défini sur un espace $(\Omega, \mathcal{B}, P)$. Nous avons vu que $X^1 + X^1$ est encore une v.a.r. sur $(\Omega, \mathcal{B}, P)$ et avec les notations du paragraphe II.4 (loi conjointe et lois marginales) on a

$$E(X^1 + X^2) = \sum_{i=1}^{p} \sum_{j=1}^{q} p_{ij}(x_i^1 + x_j^2)$$

$$= \sum_{i=1}^{p} \sum_{j=1}^{q} p_{ij} x_i^1 + \sum_{i=1}^{p} \sum_{j=1}^{q} p_{ij} x_j^2,$$

Comme $p_i^1 = \sum_{j=1}^{q} p_{ij}$ et $p_j^2 = \sum_{i=1}^{p} p_{ij}$, il vient

$$E(x^1 + x^2) = \sum_{i=1}^{p} p_i^1 x_i^1 + \sum_{j=1}^{q} p_j^2 x_j^2$$

$$= E(X^1) + E(X^2).$$

Il est d'autre part facile de voir que pour tout nombre réel α on a

$$E(\alpha X) = E(X);$$

on a donc en définitive

Théorème.

L'application $X \longrightarrow E(X)$ est une forme linéaire sur l'espace vectoriel des v.a.r. définies sur un même espace $(\Omega, \mathcal{B}, P)$.

Le produit de deux v.a.r. étant encore v.a.r. on peut calculer son espérance mathématique. Supposons que X^1 et X^2 soient indépendantes, c'est-à-dire que $p_{ij} = p_i^1 + p_j^2$ quels que soient i et j. On a alors

$$\begin{aligned} E(X^1X^2) &= \sum_{i=1}^{p}\sum_{j=1}^{q} p_{ij}x_i^1x_j^2 \\ &= \sum_{i=1}^{q}\sum_{j=1}^{q} p_i^1p_j^2x_i^1x_j^2 \\ &= \left(\sum_{i=1}^{p} p_i^1x_i^1\right) \times \left(\sum_{j=1}^{q} p_j^2x_j^2\right) = E(X^1)\,E(X^2). \end{aligned}$$

Théorème.

L'espérance mathématique du produit de deux v.a.r. indépendantes est égale au produit de leurs espérances mathématiques.

REMARQUE

Si A et B sont deux ensembles

$$E(\varphi_A\varphi_B) = E(\varphi_{A\cap B}) = P(A \cap B),$$

et si φ_A et φ_B sont indépendantes

$$E(\varphi_A\varphi_B) = E(\varphi_A)\,E(\varphi_B) = P(A)\,P(B);$$

la définition de l'indépendance de deux ensembles apparaît comme un cas particulier du théorème ci-dessus.

EXERCICE

Montrer que l'on peut avoir $E(X^1X^2) = E(X^1)\,E(X^2)$ sans que X^1 et X^2 soient indépendantes.

5. 12 VARIANCE. ÉCART-TYPE

En dehors d'un intérêt théorique et pratique très important, l'espérance mathématique a un rôle descriptif vis-à-vis des probabilités images des v.a.r. Par exemple si une v.a.r. représente les gains et les pertes dans un jeu de hasard dire que E (X) est négative c'est dire qu'on joue à un jeu désavantageux où on risque de perdre plus qu'on ne risque de gagner. Si E (X) = 0, les risques de pertes et de gains sont équilibrées. Toutefois la description d'une probabilité image par la seule donnée de l'espérance mathématique est très sommaire.

Soit par exemple une v.a.r. qui prend la valeur np avec la probabilité 1; elle a même espérance mathématique que la variable binomiale Y^n, étudiée précédemment et ces deux v.a.r. ont pourtant des probabilités images très différentes. La v.a.r. Y^n est beaucoup plus **dispersée** autour de l'espérance mathématique. Cette notion de **dispersion** est caractérisée par les nombres que nous allons définir maintenant.

Définition.

On appelle **variance** de la v.a.r. X le nombre

$$V(X) = \sum_{i=1}^{n} p_i\,(x_i - E(X))^2$$

On appelle **écart-type** ou écart quadratique le nombre $\sigma(X) = \sqrt{V(X)}$

EXEMPLE

Si X est une v.a.r. constante c'est-à-dire qui prend une valeur x avec la probabilité 1, alors $E(X) = x$ et $V(X) = 0$. Cette v.a.r. est évidemment la moins dispersée possible.

Ce nombre peut encore s'exprimer différemment. En effet $X - E(X)$, différence de X et de la v.a.r. constante égale à $E(X)$, est encore une v.a.r. et $(X - E(X))^2$ aussi; si l'on calcule l'espérance mathématique de cette nouvelle variable on voit que c'est justement $V(X)$;

$$V(X) = E[(X - E(X))^2].$$

Développons cette espérance; puisque l'espérance mathématique est une forme linéaire sur l'espace vectoriel des v.a.r. on a

$$V(X) = E(X^2) - 2E(E(X).X) + E(E(X)^2);$$

l'espérance mathématique de la v.a.r. constante $E(X)^2$ est égale à $E(X)^2$ et d'autre part à cause de la linéarité de E

$$E(E(X).X) = E(X).E(X) = E(X)^2;$$

on a donc finalement

$$V(X) = E(X^2) - E(X)^2.$$

Le nombre $E(X^2)$ s'appelle le **moment du 2e ordre de** X. Cette formule facilite souvent le calcul des variances.

EXEMPLE

La variance de la variable binomiale Y^n déjà étudiée est égale à

$$V(Y^n) = \sum_{k=0}^{n} C_n^k p^k q^{n-k} (k - np)^2;$$

expression qui n'est pas facile à calculer. Calculons plutôt

$$E[(Y^n)^2] = \sum_{k=0}^{n} C_n^k p^k q^{n-k} k^2.$$

En écrivant $k^2 = k(k-1) + k$ on obtient

$$E[(Y^n)^2] = \sum_{k=0}^{n} C_n^k p^k q^{n-k} k(k-1) + E(Y^n);$$

et $$\sum_{k=0}^{n} C_n^k p^k q^{n-k} k(k-1) = p^2 n(n-1) \sum_{k=0}^{n-2} \frac{(n-1)!}{k!(n-2-k)!} p^k q^{n-k-2}$$
$$= p^2 n(n-1)(p+q)^{n-2} = p^2 n(n-1).$$

On a donc en définitive

$$V(Y^n) = n(n-1)p^2 + np - n^2p^2$$
$$= np - np^2 = npq.$$

On obtient la dispersion maximum pour $p = q = 1/2$ et la dispersion minimum pour $q = 0$; Y^n est dans ce dernier cas la v.a.r. constante égale à n.
Le tableau ci-dessous qui donne les probabilités $P(Y^n = k)$ multipliées par 10 000 pour $n = 20$ et diverses valeurs de p illustre aussi ce phénomène.

EXERCICE

En utilisant uniquement deux décimales, tracer à partir du tableau suivant les graphes des applications $k \longrightarrow P(Y^n = k)$. Constater que pour $p = 0{,}5$ le graphe est symétrique.

k	$p = 0{,}1$	$p = 0{,}2$	$p = 0{,}3$	$p = 0{,}4$	$p = 0{,}5$
0	1 216	115	8	—	—
1	2 702	576	68	5	—
2	2 852	1 369	278	31	2
3	1 901	2 054	716	123	11
4	898	2 182	1 304	350	46
5	319	1 746	1 789	746	148
6	89	1 091	1 916	1 244	370
7	20	545	1 643	1 659	739
8	4	222	1 144	1 767	1 201
9	1	74	654	1 597	1 602
10	—	20	308	1 171	1 762
11	—	5	120	710	1 602
12	—	1	39	355	1 201
13	—	—	10	146	739
14	—	—	2	49	370
15	—	—	—	13	148
16	—	—	—	3	46
17	—	—	—	—	11
18	—	—	—	—	2
19	—	—	—	—	—
20	—	—	—	—	—

Un trait dans le tableau ci-dessus indique que la probabilité correspondante est inférieure à 1/10 000.

Le fait que la variance caractérise la dispersion apparaît également dans l'importante inégalité suivante qui porte le nom d'**inégalité de** BIENAYMÉ-TCHEBICHEFF.

Théorème.

Soit X une v.a.r. définie sur l'espace $(\Omega, \mathcal{B}, P)$. Pour tout nombre réel positif t on a

$$P(\{\omega : |X(\omega) - E(X)| > t\}) < V(X)/t^2.$$

En posant $t = u\sigma(X)$ ceci s'écrit encore

$$P(|X - E(X)| > u\sigma(X)) < 1/u^2.$$

Démonstration : on a

$$V(X) = \sum_{i=1}^{n} p_i (x_i - E(X))^2.$$

Soit I l'ensemble des i tels que $|x_i - E(X)| > t$; on a

$$V(X) = \sum_{I} p_i (x_i - E(X))^2 + \sum_{\complement_I} p_i (x_i - E(X))^2$$

$$\geqslant \sum_{I} p_i (x_i - E(X))^2 > t^2 \sum_{I} p_i$$

et $\sum_{I} p_i = P(\{\omega : |X(\omega) - E(X)| > t\})$. On a donc

$$V(X) > t^2 P(\{\omega : |X - E(X)| > t\})$$

ce qui démontre l'inégalité de BIENAYMÉ-TCHEBICHEFF.

EXERCICE

Montrer que si $V(X) = 0$, la v.a.r. est égale à $E(X)$ avec probabilité 1, ou si l'on préfère

$$P\,|\,\{\omega : X(\omega) = E(X)\}\,| = 1.$$

Si cela n'était pas vrai il existerait un nombre $r \neq E(X)$ tel que

$$P\,|\,\{\omega : X(\omega) = r\}\,| > 0.$$

On aurait donc pour $0 < t < |r - E(X)|$

$$P\,|\,\{\omega : |X(\omega) - r| > t\}\,| > 0.$$

ce qui contredit l'inégalité de Bienaymé-Tchebicheff.

COMPLÉMENT

Coefficient de corrélation. Si X^1 et X^2 sont deux v.a.r. définies sur le même espace de probabilité $(\Omega, \mathfrak{B}, P)$ on appelle ainsi le nombre

$$\rho(X^1, X^2) = \sum_{i=1}^{p} \sum_{j=1}^{q} \tilde{p}_{ij} (x_i^1 - E(X^1))(x_j^2 - E(X^2))/\sigma(X^1)\,\sigma(X^2)$$

que l'on peut encore écrire

$$\rho(X^1, X^2) = E((X^1 - E(X^1))(X^2 - E(X^2))/\sigma(X^1)\,\sigma(X^2).$$

Ce nombre est compris entre -1 et $+1$; en effet quel que soit le nombre réel λ on a

$$E(((X^1 - E(X^1)) - \lambda(X^2 - E(X^2)))^2) > 0;$$

en développant ceci signifie que le trinôme en

$$1 - 2\lambda\rho(X^1, X^2) + \lambda^2$$

est > 0 quel que soit λ, ce qui exige $\rho^2(X^1, X^2) < 1$.
Si les v.a.r. X^1 et X^2 sont indépendantes on a

$$E(X^1 - E(X^1))(X^2 - E(X^2))) = E(X^1 - E(X^1))\,E(X^2 - E(X^2)) = 0$$

puisque pour toute v.a.r. X on a $E(X - E(X)) = 0$.
Inversement si $X^2 = \alpha X^1$ pour α réel, on trouve facilement que $|\rho(X^1, X^2)| = 1$.
Dans une certaine mesure le coefficient de corrélation indique le « degré d'indépendance » de X^1 et X^2. Malheureusement il est faux que $\rho(X^1, X^2) = 0$ entraîne que X^1 et X^2 sont indépendantes.

EXERCICE

1. Construire un couple de v.a.r. non indépendantes et de coefficient de corrélation nul.
2. Montrer que l'ensemble des v.a.r. centrées définies sur un espace de probabilité $(\Omega, \mathfrak{B}, P)$ est un sous-espace vectoriel F de l'espace vectoriel H des v.a.r. Quelle est sa codimension dans H? Montrer que l'application

$$(X, Y) \longrightarrow E(XY)$$

est un produit scalaire sur F. Remarquer que la démonstration précédente est celle de l'inégalité de Schwarz pour ce produit scalaire.

V. Loi des grands nombres

5. 13 LA LOI DES GRANDS NOMBRES

Si on joue un grande nombre de fois à pile ou face, on a le sentiment que le rapport du nombre de piles obtenues au nombre total de parties doit être peu différent de 1/2. Les lois des grands nombres visent à donner une formulation rigoureuse de ce phénomène. Soit $(\Omega_n, \mathcal{B}_n, P_n)$ un espace de probabilité sur lequel on peut définier n v.a.r. X^i indépendantes et ayant toutes la même loi de probabilité. On dit alors que ces v.a.r. sont équidistribuées et l'on a

$$E(X^1) = E(X^2) = \ldots = E(X^n) \quad \text{et} \quad V(X^1) = V(X^2) \ldots = V(X_n);$$

on appellera m et σ^2 les valeurs commune de l'espérance et de la variance de X^i. On pose $Y^n = X^1 + \ldots + X^n$; calculons $E(Y^n)$ et $V(Y^n)$. Par linéarité on a

$$E(Y^n) = E(X^1) + \ldots + E(X^n) = nm;$$

d'autre part,

$$\begin{aligned} V(Y^n) &= E(X^1 + \ldots + X^n - nm^2) \\ &= \sum_{i=1}^{n} E((X^i - m)^2) + 2 \sum_{\substack{i,j=1 \\ i \neq j}}^{n} E((X^i - m)(X^j - m)); \end{aligned}$$

mais pour $i \neq j$ les v.a.r. $X^i - m$ et $X^j - m$ sont indépendantes et l'on a donc

$$E((X^i - m)(X^i - m)) = E((X^i - m) \cdot E((X^j - m) = 0$$

car $E((X^i - m)) = E(X^i) - m = m - m = 0$. On a donc finalement

$$V(Y^n) = n\sigma^2.$$

Posons alors $Z^n = Y^n/n$, par linéarité il est facile de voir que $E(Z^n) = m$ et d'autre part

$$\begin{aligned} V(Z^n) &= E((Y_n/n - m)^2) = n^{-2} E((Y_n - nm)^2) \\ &= n^{-2} V(Y^n) = n^{-1} \sigma^2. \end{aligned}$$

Appliquons à la v.a.r. Z^n l'inégalité de Bienaymé-Tchebicheff; il vient

$$P_n(|Z^n - m| > \varepsilon) < \sigma^2/n\varepsilon^2.$$

Supposons maintenant que pour chaque entier n, il existe un tel espace de probabilité $(\Omega_n, \mathcal{B}_n, P_n)$, la probabilité image des X^i restant inchangée; quel que soit ε on peut choisir n pour que $\sigma^2/n\varepsilon^2$ soit inférieure à tout nombre donné à l'avance. C'est la loi des grands nombres.

Théorème (*Loi des grands nombres*).

Dans la situation précédente, quels que soient les nombres $\varepsilon, \delta > 0$, on peut trouver n_0 tel que pour $n > n_0$

$$P_n(|Z^n - m| > \varepsilon) < \delta.$$

EXEMPLE

Dans le cas des épreuves répétées du paragraphe III.3 nous avons vu que l'on peut construire pour tout n un espace $(\Omega_n, \mathfrak{B}_n, P_n)$ sur lequel on peut définir n v.a.r. X^i indépendantes et telles que

$$P_n(X^i = 1) = p, \quad P_n(X^i = 0) = 1 - p.$$

La loi des grands nombres affirme que $Z_n = (X^1 + \ldots + X^n)/n$ « tend » vers p au sens suivant :

$\forall\, \varepsilon, \delta > 0, \exists\, n_0$ tel que $n > n_0$ entraîne $P_n(|Z_n - p| > \varepsilon) < \delta$.

REMARQUE

Plus généralement étant donnée une probabilité P sur un sous-ensemble fini de $\mathbb{R}$, on peut toujours construire des espaces $(\Omega, \mathfrak{B}_n, P_n)$ répondant aux conditions ci-dessus et tels que la probabilité image de P_n par les v.a.r. X^i soit justement P. Il suffit pour cela d'utiliser les espaces de probabilité produits. La loi des grands nombres a donc une portée tout à fait générale.

5.14 UN EXEMPLE D'APPLICATION

Un laboratoire pharmaceutique fabrique en grande quantité un médicament présenté en ampoules; une proportion p à peu près constante de ces ampoules est défectueuse. Avant de mettre les ampoules sur le marché il faut prélever une goutte dans chaque ampoule et lui faire subir un test afin de rejeter les mauvaises. Mais on peut aussi procéder de la façon suivante : on groupe les ampoules par paquets de n, on prélève une goutte dans chacune des n ampoules d'un paquet et on procède à la vérification sur le mélange de ces gouttes; si le test est négatif toutes les ampoules du paquet sont bonnes, s'il est positif, il y a au moins une des ampoules qui est mauvaise et on les teste alors séparément pour éliminer les mauvaises. Comme chaque test coûte un certain prix, il faut essayer de rendre minimum le nombre total de vérifications. Comment faut-il choisir n. Il est clair que si p est assez petit, c'est-à-dire si la fabrication n'est pas ridicule, lorsque n est petit on aura « souvent » un seul test à faire et on économisera $n - 1$ tests par rapport à la première procédure. Mais inversement si on augmente trop n, on aura « presque toujours » une ampoule mauvaise dans le lot et il faudra faire alors $(n + 1)$ tests au lieu de n. Il va donc y avoir un nombre n optimum.

Passons à la mathématisation du problème. En l'absence d'information supplémentaire, nous allons faire l'hypothèse que les ampoules sont bonnes ou mauvaises indépendamment les unes des autres. Pour un groupe donné de n ampoules nous nous trouvons alors dans le schéma binomial du paragraphe III, et nous ferons donc 1 seul test avec la probabilité $(1 - p)^n = q^n$ et $n + 1$ tests avec la probabilité $1 - q^n$. L'espérance mathématique du nombre de tests qu'il faut ainsi faire est égale à

$$q^n + (n + 1)(1 - q^n).$$

Soit X^i la v.a.r. égale au nombre de tests nécessaires pour le $i^{\text{ème}}$ paquet de n ampoules. La loi des grands nombres nous dit que si nous répétons longtemps cette procédure (ce qui est bien la situation industrielle) le nombre

$$\frac{X^1 + \ldots + X^N}{N}$$

va « tendre » vers $E(X^1) = q^n + (n + 1)(1 - q^n)$. Le rapport du nombre $X^1 + \ldots + X^N$ de tests effectués au nombre nN d'ampoules testées « tend » donc vers

$$n^{-1}(q^n + (n + 1)(1 - q^n)).$$

Il ne reste donc plus qu'à calculer le nombre n qui rend minimum l'expression ci-dessus. Nous avons fait dans ce raisonnement une hypothèse d'indépendance. Ce sera le travail du **statisticien** de vérifier que pour une production donnée cette hypothèse est acceptable et sinon de décrire comment les ampoules **dépendent** les unes des autres. Il est en effet vraisemblable que dans la réalité les ampoules mauvaises arrivent par « grappes », ce qui devrait permettre de choisir n encore plus grand; mais ceci met en jeu des mathématiques dépassant le cadre du présent programme.

5. 15 CONCLUSION SUR L'ENSEMBLE DU CHAPITRE

Le modèle que nous avons développé ne nous permet pas de répondre aux questions que nous posions tout au début du chapitre. L'espace Ω dans l'exemple étudié est trop grand. Dans quel sens faudrait-il développer le modèle pour pouvoir traiter cet exemple? On voit par exemple que l'événement {le voyageur ne repasse pas (0, 0)} est l'intersection des événements {le voyageur n'est pas en (0, 0) à l'instant n}. Il faudra donc dans la définition des tribus autoriser les réunions et intersections infinies et plus seulement finies.

Mais la notion de probabilité devra tenir compte de cette extension; si $(A_i)_{i \in I}$ est une suite infinie d'événements deux à deux disjoints il faudra pouvoir dire que

$$P\left(\bigcup_{i \in I} A_i\right) = \sum_{i \in I} P(A_i).$$

Mais qu'est-ce qu'une somme infinie de nombres réels? Comment peut-on donner un sens et une utilité à ces expressions? Ceci est l'objet de théories mathématiques qui sont développées aux niveaux suivants de l'enseignement.

EXERCICES

5.1 Soit Ω un ensemble; $\mathfrak{D}$ une partie de $\mathfrak{T}(\Omega)$ telle que
i) $\varnothing \in \mathfrak{D}$,
ii) Si A et $B \in \mathfrak{D}$ alors $A \cup B \in \mathfrak{D}$,
iii) Si A et $B \in \mathfrak{D}$ et $A \subset B$ alors $B - A \in \mathfrak{D}$.
Montrer que la classe $\mathfrak{D}$ des sous-ensembles A de Ω tels que $A \in \mathfrak{D}$ ou $\complement_\Omega A \in \mathfrak{D}$ est une tribu sur Ω.

5.2 Soit Ω_1 et Ω_2 deux ensembles et $\mathfrak{B}_1$ et $\mathfrak{B}_2$ deux tribus sur Ω_1 et Ω_2 respectivement. La classe $\mathfrak{B} \subset \mathfrak{T}(\Omega_1 \times \Omega_2)$ des parties de $\Omega_1 \times \Omega_2$ qui sont de la forme $A_1 \times A_2$ avec $A_1 \in \mathfrak{B}_1$ et $A_2 \in \mathfrak{B}_2$ est-elle une tribu?

5.3 Soit Ω un ensemble, E un sous-ensemble de Ω. Quelle est la plus petite tribu contenant la classe

$$\mathfrak{D} = \{A \mid A \in \mathfrak{T}(\Omega); \quad A \supset E\}?$$

5.4 Montrer qu'une tribu est un anneau pour les opérations Δ et $\cap$. Cet anneau a-t-il un élément unité?

5.5 Calculer le nombre de tribus différentes que l'on peut définir sur un espace Ω de cardinal n.

5.6 Sur 100 personnes interrogées au sujet de l'utilisation de deux produits A et B, 40 utilisent A, 28 utilisent B et 10 utilisent A et B. Si l'on prend au hasard une personne : parmi elles, calculer les probabilités des événements suivants :
a) x utilise l'un au moins des produits;
b) x n'utilise aucun des deux produits.

(Bacc. Aix-en-Provence, Série A.)

5.7 Étant donné un jeu de 32 cartes, quelle est la probabilité pour qu'un joueur recevant 5 cartes au hasard ait :
1° un roi?
2° au moins deux figures?
3° plus de 3 trèfles?

5.8 Une urne contient quatre boules blanches, deux noires, une rouge. On tire au hasard trois boules de l'une. Quelle est la probabilité d'avoir :
1° deux boules blanches au moins?
2° deux boules de même couleur au moins?
3° une boule de chaque couleur?

5.9 *Loi Hypergéométrique.* Soit une urne contenant N boules dont K noires et N — K blanches. On en tire n au hasard; quelle est la probabilité $p_{n,k}$ d'avoir k noires et $n - k$ blanches.

5.10 *Problème du sapeur Camembert.* On a mélangé dix paires de chaussures et l'on tire quatre chaussures au hasard. Quelle est la probabilité d'avoir :
1° au moins une paire?
2° deux paires?

5.11 On dispose de trois dés cubiques A, B et C.
Le dé A est normal; ses faces sont numérotées de 1 à 6 et elles ont toutes la même probabilité d'apparition.
Le dé B porte sur deux de ses faces le nombre 6 et sur les quatre autres le nombre 1. Toutes les faces ont la même probabilité d'apparition.
Le dé C est pipé de façon que la probabilité d'apparition de chaque face soit proportionnelle au nombre marqué sur cette face. Les faces sont numérotées de 1 à 6.

1° Quelle est la probabilité d'amener le nombre 6 en lançant une fois *a*) le dé A; *b*) le dé B; *c*) le dé C?
2° On lance les trois dés simultanément. Quelle est la probabilité d'amener *a*) trois 6; *b*) trois nombres égaux; *c*) les nombres 1, 3 et 5?
3° On lance quatre fois de suite le dé C. Quelle est la probabilité d'obtenir exactement deux fois la face marquée 6?

Donner des valeurs approchées de ces probabilités à $\frac{1}{100}$ près.

(Bacc. Bordeaux, série D.)

5.12 Le sang de tout être humain possède une caractéristique appelée facteur Rhésus. Cette caractéristique peut revêtir deux formes qu'on appelle R^+ et R^-.
Pour chacun des deux sexes, la probabilité qu'un français soit R^+ est 0,85; la probabilité qu'il soit R— est 0,15.
A. La formation d'un couple est indépendante du facteur Rhésus. Un couple étant pris au hasard, trouver les probabilités pour que
a) le mari soit R^+ et la femme R^-
b) le mari soit R^+ et la femme R^+
c) le mari soit R^- et la femme R^+
d) le mari soit R^- et la femme R^-.

B. Chez les couples où l'homme est R^+ et la femme R^- (cas *a*) il se produit dans 8 % des naissances, des accidents qui nécessitent un traitement spécial du nouveau-né. Déterminer la probabilité *p*, pour qu'un nouveau-né, de parents français dont on ne connaît pas la nature du facteur Rhésus doive subir ce traitement.
C. Dans une maternité il y a en moyenne 20 naissances par semaine.
Déterminer la probabilité pour qu'au cours d'une semaine prise au hasard k nouveau-nés doivent subir ce traitement spécial ($0 \leqslant k \leqslant 20$).
Quelle est la loi de probabilité de la variable aléatoire k?
Calculer Pr ($k = 0$) et Pr ($k = 1$).
Quelle est la probabilité pour qu'il se présente plus d'un cas à traiter durant une même semaine?
N.B. Les calculs de la question C seront effectués en utilisant la table des logarithmes décimaux.

(Bacc. Lille, série B.)

5.13 Un étang contient un nombre N, inconnu mais défini de poissons. L'objet du problème est de proposer une évaluation de N, basée sur des hypothèses bien définies.
1° On pêche dans différents endroits de l'étang; on en sort 20 poissons que l'on marque et que l'on remet vivants dans l'étang après avoir été marqués.
Quelques jours plus tard, on effectue une nouvelle pêche dans des endroits variés du même étang en rejetant à l'eau les poissons pêchés, après avoir noté s'ils sont marqués ou non. On prend ainsi 50 poissons dont 4 sont marqués.
On suppose qu'entre les deux pêches, la population de l'étang n'a pas varié et que lors de la seconde pêche à chaque coup il y a équiprobabilité de sortie pour chacun des N poissons de l'étang.
Avant la seconde pêche, on pouvait se poser le problème : quelle est la probabilité de sortir k poissons marqués sur les 50 pêchés? Répondre à cette question en donnant l'expression générale de P ($X = k$) où X désigne la variable aléatoire « nombre de poissons marqués que l'on peut sortir sur 50 poissons pêchés ».
2° Soit f, la fonction qui à x réel supérieur à 20 associe le nombre réel

$$\left(\frac{20}{x}\right)^4 \left(1 - \frac{20}{x}\right)^{46}.$$

Montrer que f a un maximum. Pour quelle valeur a de x ce maximum est-il atteint?
3° Si l'on admet que l'événement $X = 4$ qui est réalisé correspond à l'événement de probabilité maximale parmi tous les événements possibles $X = k$, $k = 0, \ldots, 50$, quelle valeur doit-on attribuer à la population N de l'étang?
Cette hypothèse conduit à la même conclusion qu'une autre hypothèse très simple que l'on aurait pu faire pour évaluer N. Laquelle?

(Bacc. Rennes, série D.)

Commentaire : *Les raisonnements ci-dessus sont typiques de la statistique mathématique dont un des objets est l'estimation de paramètres inconnus.*

5.14 *a*) Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité et A_1, A_2, A_3 trois éléments de $\mathcal{B}$; montrer que

$$P(A_1 \cup A_2 \cup A_3) = P(A_1) + P(A_2) + P(A_3) - P(A_1 \cap A_2) - P(A_2 \cap A_3) - P(A_3 \cap A_1) + P(A_1 \cap A_2 \cap A_3).$$

b) Une personne écrit à 3 correspondants différents des lettres personnelles et met les lettres au hasard dans les enveloppes portant les adresses. Quelle est la probabilité pour qu'une lettre au moins parvienne à son destinataire?

*c**) Généraliser les questions 1° et 2° à un nombre quelconque d'événements et de correspondants. La probabilité qu'une lettre au moins parvienne à son destinataire tend-elle vers zéro lorsque le nombre total des correspondants tend vers l'infini? Qu'en pensez-vous a priori?

5.15 Dans une course automobile, il y a 50 voitures engagées, dont on considère au départ qu'elles ont des chances égales.

Un propriétaire possède 10 de ces voitures numérotées de 1 à 10.

a) Quelle est la probabilité pour que les voitures 1, 2 et 3 soient respectivement première, deuxième et troisième? Quelle est la probabilité pour que les voitures 1, 2 et 3 soient les trois premières sans préciser l'ordre?

b) Quelle est la probabilité pour que les trois premières voitures arrivées appartiennent à ce propriétaire?

5.16 Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité et A et B deux événements tels que $P(A) = P(B) = a > 1/2$. Peut-on minorer la probabilité $P(A \cap B)$?

5.17 *a*) Soient P et P′ deux probabilités sur le même espace probabilisable $(\Omega, \mathcal{B})$. Montrer qu'en posant, pour $A \in \mathcal{B}$, et $\alpha \in [0, 1]$

$$Q_\alpha(A) = \alpha P(A) + (1 - \alpha) P'(A), \tag{1}$$

on définit une nouvelle probabilité sur $(\Omega, \mathcal{B})$.

Plus généralement si $P_1, P_2, \ldots, P_n$ sont n probabilités sur $(\Omega, \mathcal{B})$.

$$Q(A) = \alpha_1 P_1(A) + \ldots + \alpha_n P_n(A) \tag{2}$$

où $\alpha_1 + \alpha_2 + \ldots + \alpha_n = 1$ définit une nouvelle probabilité sur $(\Omega, \mathcal{B})$.

*b**) On suppose que $\mathcal{B}$ est engendrée par la partition $\{B_1, B_2, \ldots, B_n\}$ de Ω. On dit que Q est une probabilité extrémale si on ne peut trouver deux probabilités P et P′ et $\alpha \in]0, 1[$ tels que la relation (1) ait lieu. Si Q et Q′ sont deux probabilités extrémales distinctes, montrer qu'il existe un ensemble $A \in \mathcal{B}$ tel que $Q(A) = 1$ et $Q'(\complement A) = 1$. Trouver toutes les probabilités extrémales $P_1, \ldots, P_n$ et montrer que toute probabilité peut se mettre sous la forme (2) avec les P_i extrémales.

5.18 Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité fini et A un ensemble de $\mathcal{B}$. On appelle $\mathcal{B}_A$ la classe des ensembles de la forme $C = A \cap B$ où B décrit $\mathcal{B}$.

a) Montrer que $(A, \mathcal{B}_A)$ est un espace probabilisable.

b) Pour $C = A \cap B$ on pose

$$\tilde{P}(C) = P(A \cap B)/P(A).$$

Montrer que $(A, \mathcal{B}_A, \tilde{P})$ est un espace de probabilité.

c) Soit l'espace $(\Omega, \mathcal{P}(\Omega), P)$ représentant le jet de deux dés et A l'événement : la somme des points marqués est égale à 5. Comment peut-on décrire l'espace $(A, \mathcal{B}_A, \tilde{P})$ correspondant?

5.19 Soit f une application mesurable de $(\Omega_1, \mathcal{B}_1)$ dans $(\Omega_2, \mathcal{B}_2)$, g une application mesurable de $(\Omega_2, \mathcal{B}_2)$ dans $(\Omega_3, \mathcal{B}_3)$; montrer que l'application composée $g \circ f$ est mesurable.

5.20 Soit $(\Omega, \mathcal{B})$ un espace probabilisable tel que $\mathcal{B}$ soit engendrée par une partition $(B_1, B_2, \ldots, B_n)$ de Ω. Soient φ_i les v.a.r égales à 1 sur B_i et à zéro sur $\complement B_i$. Montrer que toutes les v.a.r sur $(\Omega, \mathcal{B})$ sont des combinaisons linéaires des φ_i. Quelle est la dimension de l'espace vectoriel des v.a.r sur $(\Omega, \mathcal{B})$?

5.21** Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité et $\mathcal{C}$ une tribu continue dans $\mathcal{B}$.

a) Montrer que les v.a.r mesurables par rapport à $\mathcal{C}$ sont mesurables par rapport à $\mathcal{B}$.

b) Montrer que pour toute v.a.r X, il existe une v.a.r $\mathcal{C}$-mesurable et notée $E(X \mid \mathcal{C})$ telle que

$$(\forall C \in \mathcal{C}) \quad E(\varphi_C . X) = E(\varphi_C . E(X \mid \mathcal{C}))$$

où φ_C est la v.a.r qui prend la valeur 1 pour $\omega \in C$ et 0 pour $\omega \in \complement C$. Montrer que

$$E(E(X \mid \mathcal{C})) = E(X).$$

c) A quoi est égal $E(X \mid \mathcal{C})$ si X est $\mathcal{C}$-mesurable? Si X est quelconque et si Y est $\mathcal{C}$-mesurable montrer que

$$E(X.Y \mid \mathcal{C}) = Y.E(X \mid \mathcal{C}).$$

d) Montrer que l'application $X \to E(X \mid \mathcal{C})$ est une application linéaire surjective de l'espace vectoriel des v.a.r mesurables par rapport à $\mathcal{B}$ sur l'espace vectoriel des v.a.r mesurables par rapport à $\mathcal{C}$. A quelle condition est-elle injective?

5.22* Soit $(\Omega, \mathcal{B})$ un espace probabilisable et $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_n$ une suite finie de tribus contenues dans $\mathcal{B}$ et telles que

$$\mathcal{B}_0 \subset \mathcal{B}_1 \ldots \subset \mathcal{B}_n \subset \mathcal{B}.$$

on appelle temps d'arrêt une v.a.r T sur $(\Omega, \mathcal{B})$ telle que $T(\Omega) \subset \{0, 1, \ldots, n\}$ et que, pour tout p de $[1, n]$,

$$\{\omega : T(\omega) = p\} \in \mathcal{B}_p$$

a) Si $T(\omega) = p$ $(0 \leqslant p \leqslant n)$ pour tout $\omega \in \Omega$, T est un temps d'arrêt. Si T et S sont deux temps d'arrêt, inf (S, T) et sup (S, T) sont encore des temps d'arrêt.
b) Soit T un temps d'arrêt et $\mathcal{B}_T$, la classe des éléments A de $\mathcal{B}$ tels que, pour tout p de $[1, n]$,

$$A \cap \{\omega : T(\omega) = p\} \in \mathcal{B}_p,$$

est une tribu sur Ω, contenue dans $\mathcal{B}$. Montrer que si $T = p$ on a $\mathcal{B}_T = \mathcal{B}_p$ et que si S est un temps d'arrêt tel que, pour tout ω, $S(\omega) \leqslant T(\omega)$ on a $\mathcal{B}_S \subset \mathcal{B}_T$.
c) Montrer que T est mesurable par rapport à $\mathcal{B}_T$.

5.23 Soit X une v.a.r telle que $X(\Omega) = \{0, 1, \ldots, n\}$ et pour tout $i \in X(\Omega)$

$$P(X = i) = \frac{1}{n+1}.$$

Calculer la moyenne, la variance et l'écart-type de X.

5.24 Construire une v.a.r de moyenne 1 et de variance 2.

5.25 On jette deux dés non truqués. Soient X et Y les v.a.r égales aux points marqués. Trouver l'espérance mathématique et la variance $X + Y$.

5.26 On considère 5 parties successives de pile ou face. On appelle « série de faces » les groupes de faces obtenues successivement. Ainsi la suite FPFFF contient deux séries de faces l'une de longueur 1 et l'autre de longueur 3. Soient X, Y, Z les v.a.r égales respectivement au nombre de faces, au nombre de séries de faces, et à la longueur de la plus longue série de faces.
1° Trouver les lois conjointes des couples (X, Y), (X, Z) et (Y, Z).
2° Trouver les lois de probabilité des v.a.r $X + Y$ et XY.
3° Calculer les moyennes et les variances de X, Y et Z.

5.27 Une v.a.r X est dite symétrique si, pour tout x de $X(\Omega)$, on a $-x \in X(\Omega)$ et si

$$P(X = x) = P(X = -x).$$

Montrer que dans ce cas X est centrée. La réciproque est-elle vraie?

5.28* Pour un groupe de n personnes, montrer que l'espérance mathématique du nombre de jours de l'année qui sont anniversaires d'exactement k personnes est $C_n^k . (365)^{1-n} (364)^{n-k}$. On suppose que l'année a 365 jours et que toutes les dispositions possibles sont équiprobables.

Commentaire : *Lorsqu'on demande de calculer des espérances mathématiques il n'est pas toujours nécessaire de calculer les lois de probabilités correspondantes; on peut utiliser la linéarité de* E. *Ainsi on pourra ici envisager les variables* X^i *égales à 1 si le* i^e *jour de l'année est l'anniversaire de k personnes exactement et à o sinon.*

5.29 Une ville comprend n pâtés de maisons dont n_j ont exactement x_j habitants ($n_1 + n_2 + \ldots = n$). On pose $m = (\Sigma\, n_j x_j)\, n$ et $a^2 = ((\Sigma\, x_j x_j^2)/n) - m^2$. On tire au hasard r pâtés et dans chacun on compte les habitants $X_1, \ldots, X_r$. Montrer que

$$E(X_1 + X_2 + \ldots + X_r) = mr,$$

et que

$$V(X_1 + X_2 + \ldots + X_r) = a^2\, r\,(n - r)/(n - 1).$$

Commentaire : *ce genre de question se rencontre dans la théorie et la pratique des sondages.*

5.30 Soient $X_1, X_2, \ldots, X_n$ n v.a.r indépendantes et équidistribuées. On appelle $\overline{X}$ la nouvelle v.a.r égale à $\dfrac{X_1 + X_2 + \ldots + X_n}{n}$. Montrer que

$$E\left(\sum_{k=1}^{n} (X_k - \overline{X})^2\right) = (n - 1)\, V(X_1).$$

Commentaire : *Cette formule intervient fréquemment en statistique mathématique.*

5.31 Soit X une v.a.r à valeurs entières ($X(\Omega) \subset \mathbb{N}$), on pose $p_n = P(X = n)$ et pour s réel

$$f_X(s) = \sum_{n \in X(\Omega)} p_n s^n.$$

La fonction f_X est donc une fonction polynôme et l'on a $f_X(1) = 1$.
a) Calculer f_X pour une variable binomiale.
b) A quoi est égal $f_X'(1)$ où f_X' est la dérivée de f_X? Calculer V(X) en fonction de f_X.
c) Si X et Y sont deux v.a.r indépendantes à valeurs entières calculer f_{X+Y} en fonction de f_X et f_Y. Énoncer le théorème ainsi démontré. Ce théorème a-t-il une réciproque?

Commentaire. *Le théorème démontré en 3° est un cas particulier d'un théorème très général qu'on retrouve et qu'on utilise dans plusieurs branches des mathématiques.*

5.32 Soit X une v.a.r, avec les notations du cours on appelle moments d'ordre k de X les nombres

$$E(X^k) = \sum_{i=1}^{n} p_i x_i^k$$

et moments factoriels d'ordre k, les nombres

$$E(X(X - 1) \ldots (X - k + 1)) = \sum_{i=1}^{n} p_i x_i (x_i - 1) \ldots (x_i - k + 1).$$

Écrire les relations liant les uns aux autres.

5.33 Urne de Polya : Une urne contient a boules rouges et b boules bleues. On tire une boule au hasard puis on la remet dans l'urne en ajoutant c boules de la couleur de la boule tirée. On tire une deuxième boule et soit X_i ($i = 1, 2$) les v.a.r égales à 1 si la boule tirée au i tirage est rouge et à zéro si non. Dresser le tableau des lois conjointes et marginales du couple (X_1, X_2). Calculer les espérances mathématiques $E(X_1)$ et $E(X_2)$.
On peut ajouter à nouveau c boules de la couleur de la 2e boule et faire un troisième tirage. Décrire la probabilité image du système (X_1, X_2, X_3). Quelle est la loi de probabilité de X_3? Comparer avec celle de X_1. Calculer $E(X_3)$.

Commentaire. *Ce schéma peut être considéré comme un modèle rudimentaire des phénomènes d'épidémie.*

5.34* *Problème de la boîte d'allumettes de* BANACH. Un mathématicien porte une boîte d'allumettes dans sa poche gauche et une dans sa poche droite. Lorsqu'il veut fumer il choisit une des poches au hasard. Les boîtes contenaient au départ N allumettes. Lorsque le mathématicien découvre qu'une des boîtes est vide, l'autre boîte peut contenir 0, 1, ... N allumettes. Ce nombre est une v.a.r dont on demande de calculer la loi de probabilité. (Le mathématicien ne découvre pas que la boîte est vide en utilisant la dernière allumette, mais au tirage suivant de cette boîte).

5.35 Un marchand d'appareils ménagers vend le même jour quatre réfrigérateurs identiques garantis pour cinq ans. La probabilité pour qu'un réfrigérateur de ce type n'ait pas de panne pendant la période de garantie est 0,9. Calculer la probabilité

1° pour que ces quatre réfrigérateurs n'aient pas de panne pendant la période de garantie;

2° pour que deux réfrigérateurs et deux seulement tombent en panne pendant la période de garantie.

On donnera les résultats avec quatre décimales.

(Bacc. Orléans, série D.)

Commentaire. *Dans cet énoncé il est sous-entendu que les réfrigérateurs tombent en panne indépendamment les uns des autres. Cette hypothèse essentielle est souvent passée sous silence dans les exercices de ce type.*

5.36 On jette deux dés. Soit A l'événement : la somme des chiffres indiqués est impaire, B l'événement au moins un est un as. Exprimer les événements $A \cap B$, $A \cup B$, $A \cap \complement B$ et calculer leurs probabilités. Les événements A et B sont-ils indépendants?

5.37 Soit $(\Omega, \mathcal{T}(\Omega), P)$ un espace de probabilité fini où P est uniformément répartie ($P(A) = \text{card } A/\text{card } \Omega$) et où card Ω est un nombre premier. Trouver tous les couples (A, B) d'événements indépendants.

5.38 Deux personnes jouent à pile ou face n fois chacune. Quelle est la probabilité quelles aient le même nombre de faces.

5.39 Soient X et Y deux v.a.r indépendantes de fonction de répartition F et G. Trouver les fonctions de répartition des v.a.r inf (X, Y) et sup (X, Y).

5.40 Soit $(\Omega, \mathcal{B}, P)$ un espace de probabilité et A, B, C trois éléments de $\mathcal{B}$. Montrer que les relations

$$P(A \cap B \cap C) = P(A).P(B).P(C),$$
$$P(A \cap B) = P(A).P(B),$$
$$P(A \cap C) = P(B).P(C),$$
$$P(A \cap C) = P(A).P(C),$$

suffisent à entraîner l'indépendance de A, B et C.

b) Soit l'espace associé au jet de deux dés non truqués. En considérant les événements

A : on obtient un nombre pair avec le premier dé,
B : on obtient un nombre pair avec le second dé,
C : la somme des nombres obtenus est paire,

montrer que trois des relations ci-dessus peuvent être satisfaites sans que la quatrième le soit. Cet exemple montre aussi que l'on peut avoir trois événements qui ne sont pas indépendants et tels que deux quelconques d'entre eux soient indépendants.

5.41 Soient $X_1, \ldots, X_n$ des v.a.r définies indépendantes ayant toutes la même distribution

$$P(X_i = k) = 1/N$$

pour $k = 1, 2, \ldots, N$. Trouver les lois de probabilités des v.a.r U_n égale à la plus grande des v.a.r X_i et V_n égale à la plus petite. Comment évoluent ces lois de probabilités lorsque n augmente?

5.42 Soit X une v.a.r définie sur un espace $(\Omega, \mathcal{B}, P)$ et f une fonction monotone et croissante de $\mathbb{R}_+$ dans $\mathbb{R}_+$.

a) Montrer que l'application $Y : \omega \to f(|X(\omega)|)$ est encore une v.a.r.

b) Montrer que pour tout nombre réel positif t, on a

$$P(|X| > t|) < E(Y)/f(t).$$

Quel résultat du cours généralise-t-on ainsi?

5.43 On considère l'ensemble $E = \{0, 1, 2, \ldots, 9\}$ des dix premiers entiers naturels. Une machine en tire au hasard; on admet que les probabilités de chacun d'eux sont égales, de sorte que, si le nombre fourni par la machine dans une expérience est X, cette variable aléatoire suit la loi de probabilité suivante :

« quel que soit a, avec $a \in E$, la probabilité pour X d'être égal à a est $\frac{1}{10}$ ».

1° Calculer l'espérance mathématique m_x de X, sa variance v_x et, à 0,0 près son écart quadratique σ_x.

2° On admet qu'après un nombre quelconque de tirages, la machine peut continuer à tirer un nombre de E, indépendamment des tirages qu'elle a faits antérieurement. Si donc $X_1, \ldots, X_n$ sont les nombres donnés dans n tirages successifs, quelle que soit la suite $(a_1, a_2, \ldots, a_n)$ de n nombres de E, la probabilité de l'événement

$$(X_1 = a_1 \text{ et } X_2 = a_2 \ldots \text{ et } X_n = a_n)$$

est $\frac{1}{10^n}$.

On considère alors la variable aléatoire

$$Z = \frac{X_1 + X_2 + \ldots + X_n}{n}.$$

Quels sont son espérance mathématique e_z, sa variance v_z, sont écart quadratique σ_z? Donner en fonction de n (inégalité de Brenaymé-Tchebitcheff) une inégalité concernant $P_n = \text{Prob}(|Z - e_z| < 1/2)$; déterminer n_0 tel que pour $n \geqslant n_0$, on ait certainement $P_n < 0{,}01$.

3° On ne fait fonctionner la machine que deux fois; elle fournit ainsi les nombres X et Y; soit T la variable aléatoire donnée par $T = X + Y$.

a) Calculer Prob $(T < 5)$.

b) Quel est l'ensemble E′ des valeurs que T est susceptible de prendre? Quelle est la loi de probabilité de T, c'est-à-dire les nombres

$$p_k = \text{Prob}(T = t_k) \quad \text{pour} \quad t_k \in E'?$$

4° Dans les mêmes conditions (deux fonctionnements de la machine); on désigne par U le plus petit et par V le plus grand des deux nombres entiers.

a) Les variables aléatoires U et V sont-elles indépendantes?

b) Quelles sont la loi de probabilité de V et son espérance mathématique?

5° Enfin on fait fonctionner la machine trois fois; on appelle W le plus grand des nombres sortis. Calculer la probabilité de l'événement $W = 9$.

Remarques. 1° Il n'est pas nécessaire d'avoir traité la question 2° pour faire les suivantes.
2° Les candidats pourront utiliser les formules rappelées ci-dessous :

$$\sum_{p=1}^{n} p = 1 + 2 + \ldots + n = \frac{n(n+1)}{2}$$

$$\sum_{p=1}^{n} p^2 = 1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

si cela leur paraît commode; mais cet emploi n'est nullement indispensable.

(Bacc. 1970, série B.)

ANNEXE A

Lois de composition interne.

Chaque fois que nous avons rencontré des notions concernant les lois internes nous les avons mises en évidence, qu'il s'agisse de notions déjà vues en Seconde et Première ou de notions ne figurant pas explicitement au programme de ces classes.
Cette manière de faire, conforme au préambule des programmes des classes de Terminales scientifiques, entraîne une dispersion dans la présentation de ces notions au cours des chapitres 1, 2 et 3. Nous avons cru rendre service au lecteur en regroupant ces notions dans la présente annexe. Nous pensons que cette deuxième présentation de ces définitions dans un ordre systématique soulagera la mémoire des élèves et leur fera sentir la profonde unité de l'algèbre.

Nous n'avons pas cru procéder de même pour l'algèbre linéaire, *car une révision systématique — avec quelques compléments — des notions d'espace vectoriel et d'application linéaire a été présentée dans la section I du chapitre 4.*

A. 1 LOI INTERNE DÉFINIE SUR UN ENSEMBLE E

a) Définitions.

On appelle **loi interne définie sur E** toute application de $E \times E$ dans E.
L'image du couple (x, y) est appelée le **composé** des **termes** x et y; il se note en séparant x et y avec un signe tel que $\star$, $\top$, $\perp$, etc.
Si le composé de x et y est noté $x + y$ on dit que la loi interne est une *addition*, ou encore qu'elle est notée *additivement*; $x + y$ est la *somme* des *termes* x et y.
Si le composé de x et y est noté $x \times y$ ou $x.y$ ou simplement xy, on dit que la loi interne est une *multiplication*, ou encore qu'elle est *notée multiplicativement*; xy est appelé le *produit* des *facteurs* x et y.
L'ensemble E muni de la loi interne notée $\star$ est représenté par $(E, \star)$. L'ensemble E muni des lois internes notées respectivement $\star$ et $\top$ est représenté par $(E, \star, \top)$.
L'unicité du composé de x et y entraîne que, quels que soient x, y, z de E

$$(x = y) \Longrightarrow (z \star x = z \star y),$$
$$(x = y) \Longrightarrow (x \star z = y \star z).$$

b) Propriétés concernant les lois internes définies sur E.

La loi interne sur E notée $\star$ est **commutative** si et seulement si, quels que soient x et y de E

$$x \star y = y \star x.$$

Elle est **associative** si et seulement si, quels que soient x, y, z de E

$$(x \star y) \star z = x \star (y \star z).$$

Elle possède un **élément neutre** si et seulement s'il existe e de E tel que, quel que soit x de E

$$e \star x = x \star e = x.$$

Si pour $(E, \star)$ il existe un élément neutre, *cet élément neutre est unique.*
Lorsque la loi est notée *additivement* (resp. *multiplicativement*) l'élément neutre, s'il existe, est appelé *élément zéro* (resp. *élément unité*).
On dit que la loi interne notée $\top$ est **distributive à gauche** par rapport à la loi interne notée $\star$, toutes deux définies sur E, si et seulement si, quels que soient x, y, z de E

$$x \top (y \star z) = (x \top y) \star (x \top z).$$

La loi T est **distributive à droite** par rapport à la loi $\star$ si et seulement si, quels que soient x, y, z de E

$$(y \star z) \top x = (y \top x) \star (z \top x).$$

Si la loi T est *commutative*, les deux identités précédentes sont équivalentes, on dit simplement que la loi $\top$ est **distributive** par rapport à la loi $\star$.

c) Propriétés concernant certains éléments de (E, $\star$).

On dit que a de E est **régulier à gauche** (resp. à **droite**) si et seulement si, quels que soient x et y de E

$$(a \star x = a \star y) \Longrightarrow (x = y)$$
$$\text{resp.} \quad (x \star a = y \star a) \Longrightarrow (x = y)).$$

Si la loi $\top$ est *commutative*, les deux propriétés ci-dessus se confondent : on dit que a est **régulier.**

La loi interne $\star$ définie sur E possédant l'élément neutre e on dit que a de (E, $\star$) est **symétrisable** si et seulement s'il existe a' de E tel que

$$a \star a' = a' \star a = e.$$

Si la loi notée $\star$ est associative, l'élément a', s'il existe, est unique : on dit que a' est le **symétrique** de a. Dans ces conditions le symétrique de a' est a : on dit que a et a' sont des **éléments symétriques** de (E, $\star$).

Lorsque *la loi est notée additivement*, le symétrique de a, s'il existe, est appelé *opposé* de a et se note $-a$.

Lorsque *la loi est notée multiplicativement* le symétrique de a, s'il existe, est appelé *inverse* de a et se note a^{-1}.

On dit que a et b sont deux **éléments permutables** de (E, $\star$) si et seulement si

$$a \star b = b \star a.$$

A. 2 GROUPES, ANNEAUX, CORPS COMMUTATIFS

a) Groupes.

On dit que (G, $\star$) est un **groupe** si et seulement si

G_1. La loi interne est *associative.*
G_2. La loi interne possède un *élément neutre.*
G_3. *Tout élément de* G *est symétrisable.*

Si on a de plus

G.C. *La loi interne est commutative*

on dit que (G, $\star$) est une **groupe commutatif** ou encore un **groupe abélien.**

b) Anneaux.

On dit que (A, +, $\times$) est un **anneau** si et seulement si

I. (A, +) est un *groupe commutatif.*
II. La *multiplication* est *associative.*
III. La *multiplication* est *distributive à droite et à gauche* par rapport à l'*addition.*

L'élément neutre de l'addition est appelé l'*élément zéro* de l'anneau; on peut le noter 0_A.
Si la *multiplication* est *commutative* on dit que (A, +, $\times$) est un **anneau commutatif.**
Si la multiplication possède un élément neutre e, on dit que (A, +, $\times$) est un **anneau unitaire.**
L'élément e est appelé *élément-unité* de l'anneau.
On dit que l'élément a est un **diviseur de zéro** de l'anneau A si $a \neq 0_A$ et s'il existe $b \neq 0_A$ tel que $ab = 0_A$.
Tout anneau *commutatif dépourvu de diviseurs de zéro* est appelé **anneau intègre.**

c) Corps commutatifs.

On dit que (K, +, $\times$) est un **corps commutatif** si et seulement si

I. (K, +, $\times$) est un anneau commutatif.
II. (K*, $\times$) est un groupe, K* désignant $K - \{0_K\}$.

Pour que l'anneau commutatif unitaire K, où les éléments zéro et unité sont respectivement 0_K et e, soit un corps, il faut et il suffit que $0_K \neq e$ et que *tout élément de* $K^* = K - \{0_K\}$ soit *inversible*.

A. 3 PARTIE STABLE. LOI INDUITE. SOUS-GROUPES. SOUS-ANNEAUX. SOUS-CORPS

a) Partie stable. Loi induite.

On dit que S est une **partie stable** de E pour la loi interne définie sur E, notée $\star$, si et seulement si, quels que soient x et y de S, on a $x \star y \in S$.
On définit ainsi une loi interne sur S (application de $S \times S$ dans S) appelée **loi induite** sur S par la loi définie sur E. En général il n'y a aucun inconvénient à noter la loi induite sur une partie stable de E par le même symbole que la loi interne sur E.
On dit aussi que la loi définie sur E **prolonge** la loi ainsi définie sur S.
On dit que S est une partie stable de $(E, \star, \top)$ si et seulement si S est une partie stable de $(E, \star)$ et de $(E, \top)$.

b) Sous-groupes d'un groupe $(G, \star)$.

On dit que F est un **sous-groupe** du groupe $(G, \star)$ si et seulement si
i. F est une partie stable de $(G, \star)$.
ii. $(F, \star)$ est un groupe.
Ainsi G et $\{e\}$ (e, élément neutre de G) sont des sous-groupes de G. Tout sous-groupe de G, distinct de G et de $\{e\}$ est appelé *sous-groupe propre* de G.
Une partie F de G est un sous-groupe du groupe $(G, \star)$ si et seulement si
1. F est une partie non vide de G.
2. Quels que soient x et y de F, y' étant le symétrique de y, on a

$$x \star y' \in F.$$

En notation additive, on écrira $x - y \in F$,
En notation multiplicative, on écrira $xy^{-1} \in F$.

c) Sous anneaux d'un anneau $(A, +, \times)$.

On dit que B est un **sous-anneau** de l'anneau $(A, +, \times)$ si et seulement si
i. B est une partie stable de $(A, +, \times)$.
ii. $(B, +, \times)$ est un anneau.
Ainsi A et $\{0_A\}$ sont des sous-anneaux de $(A, +, \times)$. Tout sous-anneau de A, distinct de A et de $\{0_A\}$ est appelé sous-anneau propre de A.
Une partie B de A est un sous-anneau de l'anneau $(A, +, \times)$ si et seulement si
1. B est une partie non vide de A.
2. Quels que soient x et y de B on a $x - y \in B$.
3. Quels que soient x et y de B on a $xy \in B$.

d) Sous-corps d'un corps commutatif $(K, +, \times)$.

On dit que H est un **sous-corps** du corps commutatif $(K, +, \times)$ si et seulement si
i. H est une partie stable de $(K, +, \times)$.
ii. $(H, +, \times)$ est un corps commutatif.
Une partie H de K est un **sous-corps** du corps commutatif $(K, +, \times)$ si et seulement si
1. H est une partie non vide de K.
2. Quels que soient x et y de H on a $x - y \in H$.
3. Quels que soient x et y de H on a $xy \in H$.
4. Quel que soit x de $H^* = H - \{0_K\}$ on a $x^{-1} \in H$.

Un corps commutatif étant un anneau commutatif particulier, on dira que H est un **sous-anneau du corps commutatif** $(K, +, \times)$ si et seulement si H est un sous-anneau de $(K, +, \times)$ considéré comme anneau.

A. 4 HOMOMORPHISMES. ISOMORPHISMES

a) Homomorphismes.

Étant donnés un ensemble E muni d'une loi interne notée $\top$ et un ensemble E′ muni d'une loi interne notée $\top'$, on dit qu'une application f de E dans E′ est un **homomorphisme** de $(E, \top)$ dans $(E', \top')$ si et seulement si

$$(\forall\, (x, y) \in E \times E) \qquad f(x \top y) = f(x) \top' f(y).$$

On dira que f application de E dans E′ est un homomorphisme de $(E, \top, \bot)$ dans $(E', \top', \bot')$ si et seulement si f est à la fois un homomorphisme de $(E, \top)$ dans $(E', \top')$ et un homomorphisme de $(E, \bot)$ dans $(E', \bot')$.

b) Isomorphismes.

On appelle **isomorphisme** de $(E, \top)$ sur $(E', \top')$ tout homomorphisme f de $(E, \top)$ dans $(E', \top')$ possédant les propriétés suivantes :

i. f est une bijection.
ii. f^{-1} est un homomorphisme de $(E', \top')$ dans $(E, \top)$.

Pour que f *homomorphisme* de $(E, \top)$ dans $(E', \top')$ soit un *isomorphisme il suffit que* f soit une *bijection*. On dit alors que $(E, \top)$ et $(E', \top')$ sont **isomorphes.** Les propriétés de la loi $\top$ dans E sont exactement les mêmes que les propriétés de la loi $\top'$ dans E.
On dit que f est un isomorphisme de $(E, \top, \bot)$ sur $(E', \top', \bot')$ si et seulement si f est à la fois un isomorphisme de $(E, \top)$ sur $(E', \top')$ et un isomorphisme de $(E, \bot)$ sur $(E', \bot')$.

A. 5 GROUPES, ANNEAUX, CORPS COMMUTATIFS TOTALEMENT ORDONNÉS

a) Groupe commutatif totalement ordonné $(G, \star, \leqslant)$.

Soit un ensemble G muni à la fois d'une loi interne notée $\star$ et d'une relation d'ordre notée $\leqslant$; nous noterons cet objet mathématique $(G, \star, \leqslant)$.
On dit que $(G, \star, \leqslant)$ est un **groupe commutatif totalement ordonné** si et seulement si

i. $(G, \star)$ est un groupe commutatif.
ii. $(G, \leqslant)$ est un ensemble totalement ordonné.
iii. La loi interne $\star$ et la relation d'ordre $\leqslant$ dont compatibles, c'est-à-dire, quels que soient x, y, z de G on a

$$(x \leqslant y) \Longrightarrow (x \star z \leqslant y \star z).$$

b) Anneau (resp. corps) commutatif totalement ordonné.

Soit un ensemble A muni d'une addition, d'une multiplication et d'une relation d'ordre notée $\leqslant$; nous noterons cet objet mathématique $(A, +, \times, \leqslant)$.
On dit que $(A, +, \times, \leqslant)$ est un **anneau** (resp. **corps**) **commutatif totalement ordonné** si et seulement si

i. $(A, +, \times)$ est un anneau (resp. corps) commutatif.
ii. $(A, \leqslant)$ est un ensemble totalement ordonné.
iii. Quels que soient x, y, z de A on a

$$\textbf{O.A.} \quad (x \leqslant y) \Longrightarrow (x + z \leqslant y + z),$$
$$\textbf{O.M.} \quad (0_A \leqslant x \text{ et } 0_A \leqslant y) \Longrightarrow (0_A \leqslant xy).$$

A. 6 LOI INTERNE DÉFINIE SUR $\mathcal{F}(X, E)$ A PARTIR D'UNE LOI INTERNE DÉFINIE SUR E

Nous définirons une notion que nous avons rencontrée plusieurs fois sans jamais la systématiser.
Soit E un ensemble muni d'une loi interne notée $\top$ et X un ensemble quelconque.
On peut définir sur l'ensemble $E' = \mathcal{F}(X, E)$ de toutes les applications de X dans E une loi interne $\top'$ associée à la loi $\top$ définie sur E.
Soit f et g deux éléments quelconques de $\mathcal{F}(X, E)$ le composé $f \top' g$ est défini de la manière suivante $\qquad (\forall\, x \in X) \qquad (f \top' g)(x) = f(x) \top g(x).$

La plupart du temps il n'y a aucun inconvénient à noter la loi interne sur E et la loi interne sur $\mathcal{F}(X, E)$ par le même symbole.

EXEMPLES

1. $X = I$ intervalle de $\mathbb{R}$, $E = \mathbb{R}$; soient deux fonctions réelles f et g définies sur I, $f + g$ et fg sont définies par
$$(\forall x \in I) \qquad (f + g)(x) = f(x) + g(x)$$
$$(\forall x \in I) \qquad (fg)(x) = f(x)\, g(x).$$

2. $X = E$ espace vectoriel sur $\mathbb{R}$; soient deux applications linéaires f et g de E dans E, $f + g$ est définie par
$$(\forall x \in E) \qquad (f + g)(x) = f(x) + g(x).$$
On sait que $f + g$ est aussi une application linéaire (cf. § 4.3 d).

Si la loi $\top$ est associative et commutative sur E, il en est de même pour la loi $\top'$ sur $E' = \mathcal{F}(X, E)$. De même si e est élément neutre de $(E, \top)$, la fonction e' constante sur X et de valeur e, c'est-à-dire définie par
$$(\forall x \in X) \qquad e'(x) = e,$$
est élément neutre de $(E', \top')$. Mais il ne faudrait pas croire que *toutes* les propriétés de $(E, \top)$ sont transmises à $(E', \top')$. Par exemple $(\mathbb{R}, +, \times)$ est un *corps commutatif* et $(\mathcal{F}(I, \mathbb{R}), +, \times)$ est seulement un anneau commutatif unitaire; en particulier cet anneau possède des diviseurs de zéro (prendre $I = [a, b]$ avec $a < c < b$, f nulle sur $[a, c]$ non nulle sur $[c, b]$ et inversement g non nulle sur $[a, c]$ et nulle sur $[c, b]$; si ω est la fonction nulle sur $[a, b]$ on a
$$f \neq \omega \quad \text{et} \quad g \neq \omega \quad \text{et} \quad fg = \omega).$$

REMARQUES

1. Les considérations ci-dessus s'étendent aux lois externes. Par exemple, si E est un espace vectoriel sur $\mathbb{R}$, à toute application linéaire f de E dans E on peut associer l'application αf, définie pour tout réel α par
$$(\forall x \in E) \qquad (\alpha f)(x) = \alpha f(x).$$
On sait que αf est aussi une application linéaire. On voit sans peine que si $\mathfrak{L}(E)$ désigne l'ensemble des applications linéaires de E dans E $(\mathfrak{L}(E))$, $+$, $\bullet$) est, comme E, un espace vectoriel sur $\mathbb{R}$.

2. Dans le même ordre d'idée, si $\mathcal{R}$ est une relation binaire définie sur un ensemble E et X un ensemble quelconque on peut définir, sur $E' = \mathcal{F}(X, E)$ une relation $\mathcal{R}'$ associée à $\mathcal{R}$ en posant par définition pour tout f et g de E'
$$(f\, \mathcal{R}'\, g) \iff [(\forall x \in X) \qquad f(x)\, \mathcal{R}\, g(x)].$$
Certaines propriétés de $\mathcal{R}$ se transmettent à $\mathcal{R}'$ mais pas toutes. Par exemple on voit facilement que $(\mathbb{R}, \leqslant)$ est un *ensemble totalement ordonné* tandis que $\mathcal{F}(I, \mathbb{R})$ muni de la relation $\leqslant$ définie par
$$(f \leqslant g) \iff (\forall x \in I) \qquad f(x) \leqslant g(x)$$
est seulement un *ensemble partiellement ordonné.*
Si $I = [a, b]$ avec $a < c < b$, les fonctions f et g définies par
$$f(x) = 1 \text{ pour } a \leqslant x \leqslant c \quad \text{et} \quad f(x) = -1 \text{ pour } c < x \leqslant b$$
$$g(x) = 2 \qquad\qquad\qquad\qquad g(x) = -2$$
ne sont pas comparables pour l'ordre défini sur $\mathcal{F}(I, \mathbb{R})$.

ANNEXE B

Introduction à l'étude des cardinaux et des entiers naturels.

L'exposé suivant présente une introduction à la théorie des cardinaux. En admettant deux ou trois résultats, il permet de retrouver, en particulier, toutes les propriétés de $(\mathbb{N}, +, \times, \leqslant)$ *et des ensembles finis, admises en bloc aux paragraphes 1.3, 1.4 et 1.6 a.*
Avant d'étudier cette annexe B, le lecteur est prié de lire les paragraphes 1.1 et 1.2 qui contiennent des notions n'ayant pas été vues de manière systématique dans les classes précédentes.

B. 1 INTRODUCTION

Il existe bien des manières de présenter l'ensemble $\mathbb{N}$ des entiers naturels.
L'une des plus classiques est l'exposé axiomatique de PÉANO ou l'une de ses nombreuses variantes. L'inconvénient majeur d'un tel exposé est qu'il faut montrer que les axiomes posés sont compatibles, problème délicat qui ne trouve sa solution que dans la théorie des ensembles. D'autre part les démonstrations des propriétés de $(\mathbb{N}, +, \times, \leqslant)$ par un recours systématique au raisonnement par récurrence sont, la plupart du temps, fastidieuses.

C'est, en particulier, pour ces raisons que nous préférons présenter les grandes lignes de la construction de $\mathbb{N}$ en utilisant directement la théorie des ensembles. Notre exposé ne sera, en effet, qu'une introduction car, d'une part, nous admettrons sans démonstration deux ou trois résultats et, d'autre part, nous n'avons à notre disposition que la notion intuitive d'ensemble. Malgré ces inconvénients nous pensons que l'intérêt et la variété des notions rencontrées dans notre exposé légitime ce choix du point de vue pédagogique.

B. 2 CLASSES ET ENSEMBLES

a) Introduction.

Les paradoxes apparus très vite, à la fin du XIX^{e} siècle, dès l'invention de la théorie des ensembles par CANTOR, montrèrent que la notion intuitive d'ensemble était insuffisante. En particulier la plupart des paradoxes rencontrés provenaient de la considération illégitime de « l'ensemble de tous les ensembles ». Au cours de la première moitié du XIX^{e} siècle des théories axiomatiques des ensembles, car il y en a plusieurs, furent substituées à la théorie intuitive de CANTOR. Il n'est pas question pour nous d'indiquer, même les grandes lignes, d'une telle théorie. Nous dirons simplement que l'on est amené à distinguer les « collections quelconques » appelées *classes* et les *ensembles*. Ainsi nous parlerons de la *classe de tous les ensembles*. Dans une théorie axiomatique des ensembles un axiome indique dans quel cas et dans quel cas seulement une classe est un ensemble. Nous nous contenterons d'indiquer comment, à partir d'ensembles connus, on peut former d'autres ensembles.

b) Construction d'ensembles.

Quels que soient les ensembles X et Y nous admettrons les propriétés suivantes :

1. Il existe un ensemble appelé *réunion* de X et Y, noté $X \cup Y$ dont les éléments sont tous les éléments appartenant à X *ou* à Y.

2. Il existe un ensemble appelé *intersection* de X et Y, noté $X \cap Y$ dont les éléments sont tous les éléments appartenant à X *et* à Y.

3. Il existe un ensemble appelé *ensemble-produit* de X et Y, noté $X \times Y$, dont les éléments sont tous les couples (x, y) tels que $x \in X$ et $y \in Y$.

4. Soit $\mathcal{A}$ une propriété définie sur X, il existe un ensemble A dont les éléments sont tous les éléments de X possédant la propriété $\mathcal{A}$; A est appelé *sous-ensemble* ou partie de X.

5. Il existe un ensemble, noté $\mathcal{P}(X)$ dont les éléments sont *tous les sous-ensembles* de X.

6. Il existe un ensemble, noté $\mathcal{F}(X, Y)$, dont les éléments sont *toutes les applications* de X dans Y.

7. Si $\mathcal{R}$ est une relation d'équivalence définie sur X, il existe un ensemble appelé *ensemble-quotient* de X par $\mathcal{R}$, noté $X/\mathcal{R}$, dont les éléments sont toutes les classes d'équivalence, modulo $\mathcal{R}$.

Lorsque l'on connaît l'ensemble $\mathbb{N}$, ces propriétés permettent de montrer que $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}$ et $\mathbb{C}^n$ $(n \in \mathbb{N}^*)$, $\mathcal{F}(I, \mathbb{R})$ où $I \subset \mathbb{R}$... sont des ensembles. En particulier nous verrons à l'annexe C que $\mathbb{Z}$ est un ensemble; c'est $\dfrac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ où $\mathcal{R}$ est une relation d'équivalence définie sur $\mathbb{N} \times \mathbb{N}$; d'après les propriétés 3 et 7, $\dfrac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ est bien un ensemble.

EXERCICE

Démontrer les propriétés 6 et 7 ci-dessus à l'aide des propriétés 3, 4 et 5.

REMARQUE

Dans les introductions à certains des paragraphes suivants nous parlerons d' « ensemble fini » de « nombre d'éléments d'un ensemble fini » et ceci avant d'avoir défini au § B. 8 les ensembles finis. Il n'y a là aucun cercle vicieux, les expressions entre guillemets permettant seulement, de présenter des considérations intuitives motivant les définitions abstraites qui vont suivre.

B. 3 ÉQUIPOTENCE DES ENSEMBLES. NOTION DE CARDINAL

a) Introduction.

Lorsque nous désirons savoir si deux ensembles « finis », par exemple, dans une pièce, un ensemble S de sièges à une place et un ensemble P de personnes, ont le même « nombre d'éléments » nous pouvons procéder de deux manières :

1. Nous « comptons » les éléments de S et de P; soient s et p les « nombres entiers » obtenus : les ensembles S et P ont le même « nombre d'éléments » si et seulement si $s = p$.
2. Chaque personne cherche à s'asseoir sur un siège; les ensembles S et P ont le même « nombre d'éléments » si et seulement si, cette opération terminée, toutes les personnes sont assises et tous les sièges sont occupés.

Le premier procédé ne peut se généraliser facilement à des ensembles « infinis »; en revanche le second se généralise immédiatement à ce dernier cas : il suffit de remarquer que le procédé 2 consiste à essayer de construire une bijection de S sur P : les ensembles S et P ont le même « nombre d'éléments » et si seulement s'il existe une bijection de S sur P.

b) Relation d'équipotence.

Définition 1.

Étant donnés deux ensembles quelconques A et B, nous dirons qu'ils ont **même puissance,** ou qu'ils sont **équipotents** si et seulement si la propriété suivante est vérifiée :
Il existe une bijection de A sur B.
On écrit alors

$$A \text{ eq } B.$$

Rappelons que lorsque nous disons : il existe un objet tel que... cela signifie : il existe *au moins* un objet tel que..., lorsque nous voulons signifier que l'objet est unique nous disons : il existe un et un seul objet tel que... ou il existe un objet unique tel que...

L'énoncé non (A eq B), que l'on peut écrire (A non eq B), signifie qu'il n'existe pas de bijections de A sur B, ou encore que toutes les applications de A dans B sont non bijectives.
Si A et B sont des parties d'un ensemble E *fixé* la phrase : il existe une bijection de A sur B énonce que A et B sont liés par une relation binaire définie sur l'ensemble $\mathfrak{P}(E)$.
Or la définition donnée de l'équipotence concerne des ensembles A et B *quelconques;* nous sommes amenés à généraliser la notion de relation en disant : la relation d'équipotence est une relation binaire entre ensembles. Mais nous ne pouvons pas dire que cette relation est définie sur un ensemble, car comme nous l'avons dit plus haut, il n'existe pas d'ensemble dont tout ensemble soit élément (cf. remarque 3 à la fin du § B.6). Nous considérerons qu'il existe un objet mathématique appelé **classe de tous les ensembles,** *qui n'est pas un ensemble, mais dont les éléments sont tous les ensembles*, et nous dirons que l'énoncé :

il existe une bijection de A sur B

définit une **relation binaire sur la classe de tous les ensembles;** elle est appelée relation d'équipotence.

c) Propriétés de la relation d'équipotence.

Nous allons être amenés à généraliser les notions de réflexivité, symétrie, transitivité à la relation d'équipotence.

Quel que soit l'ensemble A, l'application Id_A est une bijection de A sur A; nous dirons encore que l'équipotence est *réflexive.*

Quels que soient les ensembles A et B, s'il existe une bijection f de A sur B, alors il existe une bijection de B sur A, à savoir f^{-1}; nous dirons que l'équipotence est *symétrique.*

Enfin quels que soient les ensembles A, B et C, s'il existe une bijection f de A sur B et une bijection g de B sur C, il existe une bijection de A sur C, à savoir $g \circ f$ car, comme vous le savez, la composée de deux bijections est une bijection; nous dirons que l'équipotence est *transitive.*

Nous sommes tout naturellement amenés à dire que la relation d'équipotence est une **relation d'équivalence** définie sur la classe de tous les ensembles.

d) Notion de cardinal.

Nous appellerons **cardinal** d'un ensemble la classe de tous les ensembles qui lui sont équipotents.
Par suite l'énoncé

card A = card B

est *synonyme* de l'énoncé

A eq B.

Nous sommes amenés à dire que tous les cardinaux constituent la *classe-quotient* de la classe de tous les ensembles par la relation d'équipotence. Nous admettrons que cette classe-quotient n'est pas un ensemble, autrement dit, qu'il n'existe pas d'ensemble dont tout cardinal soit élément. Mais nous parlerons de la **classe de tous les cardinaux,** comme nous avons parlé de la classe de tous les ensembles.

Le cardinal du *vide* $\varnothing$ est noté 0 (*zéro*).

Soit E un ensemble non vide, il comprend donc au moins un élément a; on dit que E est un *singleton* si et seulement si tout élément x de E est égal à a; on écrit $E = \{a\}$. Il est évident que tous les singletons sont équipotents; le cardinal d'un singleton est noté 1 (*un*).

De même le cardinal de toutes les **paires** $\{a, b\}$ avec $a \neq b$ est noté 2 (*deux*) etc.

EXERCICES

1. On suppose que vous connaissez l'ensemble $\mathbb{N}$ des entiers naturels.
   a) On désigne par $2\,\mathbb{N}$ l'ensemble des entiers naturels pairs; démontrer que
   $$\text{card } \mathbb{N} = \text{card } (2\,\mathbb{N}).$$
   b) On désigne par $2\,\mathbb{N} + 1$ l'ensemble des entiers naturels impairs; démontrer que
   $$\text{card } (2\,\mathbb{N} + 1) = \text{card } \mathbb{N}.$$

c) Soit $k\,\mathbb{N}$ l'ensemble des entiers naturels multiples de l'entier naturel $k > 2$, comparez

$$\text{card}\ \mathbb{N} \quad \text{et} \quad \text{card}\ (k\,\mathbb{N}).$$

d) Soit P l'ensemble des entiers naturels « carrés parfaits » comparer card $\mathbb{N}$ et card P.

2. Soit [A , B] et [A′ , B′] deux segments du plan affine tels que $A \neq B$ et $A' \neq B'$; démontrer que card [A , B] = card [A′ , B′] (on supposera d'abord que [A , B] et [A′ , B′] ne sont pas contenus dans une même droite; dans ce dernier cas on considérera un troisième segment [C , D] non colinéaire à [A , B] et à [A′, B′].

La relation (card A ≠ card B) négation de (card A = card B) signifie que A et B ne sont pas équipotents, autrement dit qu'il n'y a pas de bijection de A sur B ou encore que toutes les applications de A dans B sont non bijectives.

EXERCICE

3. Démontrer que $0 \neq 1$, $0 \neq 2$ et $1 \neq 2$.

e) Remarque fondamentale.

Si α est un cardinal, c'est-à-dire une classe d'équivalence pour la relation d'équipotence, il existe au moins un ensemble A ayant α pour cardinal; nous dirons encore que l'ensemble A est un **représentant** du cardinal α; il peut y en avoir d'autres A′, A″...

EXEMPLES :

0 a pour seul représentant $\varnothing$,

1 a pour représentant tout singleton,

2 a pour représentant toute paire $\{a, b\}$ $(a \neq b)$.

Soit α et β des cardinaux, A, A′... des représentants de α et B, B′... des représentants de β.
Pour définir une *opération* entre les cardinaux α et β il est tout naturel de se ramener à une opération entre A et B. Pour que l'opération sur α et β soit correctement définie, il faudra montrer que le cardinal du résultat de l'opération sur les ensembles reste le même lorsque l'on remplace A par A′ et B par B′ : nous dirons alors que **l'opération définie sur les ensembles A et B est compatible avec l'équipotence des ensembles.**
De même si nous voulons définir une relation entre les cardinaux α et β en utilisant une relation entre les ensembles A et B il faudra montrer que cette relation entre A et B est équivalente à la même relation entre A′ et B′; nous dirons, dans ce cas, que **la relation entre les ensembles A et B est compatible avec l'équipotence des ensembles.**

B. 4 SOMME DE DEUX CARDINAUX

a) Introduction.

Si nous avons deux ensembles » finis « *disjoints* A et B ayant respectivement $a = 3$ éléments et $b = 11$ éléments la réunion $A \cup B$ est un ensemble « fini » dont le nombre d'éléments est $a + b = 14$.

b) Définition de la somme de deux cardinaux α et β.

Soit A et B des représentants respectifs de α et β. Si A et B sont *disjoints*, nous sommes tentés de poser par définition $\alpha + \beta = \text{card}\ (A \cup B)$; cela ne sera correct (cf. § B.3 e) que, si A′ et B′ étant deux autres représentants disjoints de α et β, on a card $(A' \cup B') = (A \cup B)$. Ce résultat est exact; il existe en effet les bijections

$$f : A \longrightarrow A' \quad , \quad g : B \longrightarrow B'.$$

Considérons l'application F de $A \cup B$ dans $A' \cup B'$ définie de la manière suivante : si $x \in A \cup B$, comme $A \cap B = \varnothing$:

ou bien $x \in A$, et nous posons $F(x) = f(x)$,
ou bien $x \in B$, et nous posons $F(x) = g(x)$.

nous avons donc $F : A \cup B \longrightarrow A' \cup B'$.

Soit y un élément quelconque de $A' \cup B'$, cherchons à résoudre l'équation $F(x) = y$; comme $A' \cup B' = \varnothing$, on a les résultats suivants :

ou bien $y \in A'$ et $x = f^{-1}(y)$ (f est une bijection)
ou bien $y \in B'$ et $x = g^{-1}(y)$ (g est une bijection).

L'équation $F(x) = y$ a donc une solution unique, quel que soit y du but de F; F est donc une bijection, donc

$$\text{card}(A \cup B) = \text{card}(A' \cup B').$$

Si A et B *ne sont pas disjoints* on peut se demander s'il existe des ensembles disjoints A″ et B″ respectivement équipotents à A et B. C'est bien le cas; en effet, considérons une paire $\{0, 1\}$, par exemple, et les deux ensembles produits

$$A'' = A \times \{0\} \quad , \quad B'' = B \times \{1\}.$$

Soit $(x, y) \in A'' \cap B''$, on devrait avoir $y = 0$ et $y = 1$. Or $0 \neq 1$ (cf. § B.3 ex. 3). Donc A″ et B″ n'ont pas d'élément commun.
Il est par ailleurs évident que les applications

$$\begin{array}{ccc} A & \longrightarrow & A'' \\ x & \longmapsto & (x, 0) \end{array} \qquad \begin{array}{ccc} B & \longrightarrow & B'' \\ y & \longmapsto & (y, 1). \end{array}$$

sont des bijections. Donc les ensembles A″ et B″ sont disjoints et ont pour cardinaux respectifs $\alpha = \text{card } A$ et $\beta = \text{card } B$. Concluons :

Théorème et définition 2.

Quels que soient les cardinaux α et β, il existe des représentants disjoints A et B de α et β. Le cardinal de $A \cup B$ est indépendant des représentants disjoints A de α et B de β choisis; ce cardinal est appelé **somme** des cardinaux α et β et se note $\alpha + \beta$.
L'opération qui associe aux cardinaux α et β leur somme est appelée **addition** des cardinaux.

Donc si $\text{card } A = \alpha$, $\text{card } B = \beta$, $A \cap B = \varnothing$ on a

$$\alpha + \beta = \text{card}(A \cup B).$$

Exemple. Soit E un ensemble de cardinal α et $\{a\}$ un singleton tel que $a \notin E$ on a

$$\text{card}(E \cup \{a\}) = \alpha + 1.$$

EXERCICES

1. Démontrer que $0 + 1 = 1$, $1 + 1 = 2$.
2. Supposons connu l'ensemble $\mathbb{N}$ des entiers naturels désignons par ν son cardinal. Démontrer que $\nu + \nu = \nu$ (Utilisez les ensembles $2\,\mathbb{N}$ et $2\,\mathbb{N} + 1$ de l'exercice 1 du § B. 3).

c) Propriétés de l'addition des cardinaux.

Soient α, β, γ trois cardinaux quelconques; en considérant des représentants respectifs A, B, C de α, β, γ deux à deux disjoints et en utilisant les propriétés de la réunion des ensembles vous démontrerez sans peine les résultats suivants :

Théorème 1.

Quels que soient les cardinaux α, β, γ on a
1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$,
2. $\alpha + 0 = 0 + \alpha = \alpha$,
3. $\alpha + \beta = \beta + \alpha$.

Nous dirons que l'addition des cardinaux est *associative* et *commutative* et qu'elle a 0 pour *élément neutre*.

Quels que soient les cardinaux α, β, γ il est évident que si $\alpha = \beta$ alors $\alpha + \gamma = \beta + \gamma$.
En revanche si $\alpha + \gamma = \beta + \gamma$ on ne peut conclure $\alpha = \beta$: il suffit de considérer le contre-exemple qui résulte de l'exercice 2 ci-dessus.

Cependant nous avons le résultat suivant :

Théorème 2.

Quels que soient les cardinaux α et β on a

$$(\alpha + 1 = \beta + 1) \Longrightarrow (\alpha = \beta)$$

Soient A et B des représentants respectifs de A et B et $\{a\}$ et $\{b\}$ deux représentants de 1 tels que $a \notin A$ et $b \notin B$; nous avons

$$\text{card}(A \cup \{a\}) = \alpha + 1 = \beta + 1 = \text{card}(B \cup \{b\})$$

il existe donc une bijection f de $A \cup \{a\}$ sur $B \cup \{b\}$.

1. Si $b = f(a)$, l'application f étant bijective on a $f(A) = B$, il est évident que l'application f' de A dans B définie par

$$(\forall x \in A) \qquad f'(x) = f(x)$$

est une bijection; donc card A = card B, c'est-à-dire $\alpha = \beta$.

2. Si $b \neq f(a)$, posons $c = f(a)$; on a $c \in B$. Considérons l'application g de $B \cup \{b\}$ dans lui-même défini par

$$g(x) = x \quad \text{si} \quad x \notin \{b, c\},$$
$$g(b) = c,$$
$$g(c) = b;$$

il est évident que c'est une bijection. Considérons alors $h = g \circ f$

$$A \cup \{a\} \xrightarrow{f} B \cup \{b\} \xrightarrow{g} B \cup \{b\}.$$
$$\underbrace{\qquad\qquad\qquad\qquad}_{g \circ f}$$

L'application h, composée de deux bijections est, comme vous le savez, une bijection; or on a $h(a) = g(f(a)) = g(c) = b$; nous pouvons appliquer à h bijection de $A \cup \{a\}$ sur $B \cup \{b\}$ vérifiant $h(a) = b$ le procédé appliqué à la bijection f dans le cas 1.
Nous avons donc montré dans tous les cas que, si $\alpha + 1 = \beta + 1$, alors $\alpha = \beta$.

B. 5 PRODUIT DE DEUX CARDINAUX

a) Définition du produit de deux cardinaux α et β.

Soit A et B des représentants respectifs de α et β; nous sommes tentés de poser par définition $\alpha.\beta = \text{card}(A \times B)$; cela ne sera correct (cf. § B.3 e) que si, A' et B' étant deux autres représentants respectifs de α et β, on a $\text{card}(A' \times B') = \text{card}(A \times B)$. Ce résultat est exact, il existe en effet les bijections :

$$f : A \longrightarrow A' \quad , \quad g : B \longrightarrow B'.$$

Si $(x, y) \in A \times B$ alors $x \in A$, $y \in B$ et $f(x) \in A'$, $g(y) \in B'$; considérons l'application

$$G : A \times B \longrightarrow A' \times B'$$
$$(x, y) \longmapsto (f(x), g(x)).$$

Quel que soit (x', y') de $A' \times B'$ l'équation $G(x, y) = (x', y')$ c'est-à-dire

$$(f(x), g(y)) = (x', y'),$$

ou encore

$$f(x) = x' \quad \text{et} \quad g(y) = y'$$

a une solution unique $(x, y) = (f^{-1}(x'), g^{-1})(y)$ car f et g sont bijectives. Donc G est une bijection. Concluons :

Théorème et définition 3.

Quels que soient les cardinaux α et β ayant pour représentants respectifs les ensembles A et B, le cardinal de $A \times B$ est indépendant des représentants A de α et B de β choisis; ce cardinal est appelé **produit** des cardinaux α et β et se note $\alpha.\beta$ ou $\alpha\beta$.
L'opération qui associe aux cardinaux α et β leur produit $\alpha\beta$ est appelée **multiplication** des cardinaux.

Donc si card A $= \alpha$, card B $= \beta$ on a

$$\alpha\beta = \text{card}\,(A \times B).$$

b) Propriétés de la multiplication des cardinaux.

Le lecteur est prié de résoudre les exercices suivants.

EXERCICES

1. Quels que soient les ensembles A, B et C, démontrer que l'application

$$\begin{array}{ccc} ((A \times B), C) & \longrightarrow & (A \times (B \times C)) \\ ((x, y), z) & \longmapsto & (x, (y, z)) \end{array}$$

est bijective.

2. Quel que soit l'ensemble A, démontrer que les applications

$$\begin{array}{ccc} A & \longrightarrow & A \times \{1\} \\ x & \longmapsto & (x, 1) \end{array} \qquad \begin{array}{ccc} A & \longrightarrow & \{1\} \times A \\ x & \longmapsto & (1, x) \end{array}$$

sont des bijections.

3. Quels que soient les ensembles A et B, démontrer que l'application

$$\begin{array}{ccc} A \times B & \longrightarrow & B \times A \\ (x, y) & \longmapsto & (y, x) \end{array}$$

est bijective.

4. Démontrer que, quels que soient les ensembles, A, B et C, on a

$$C \times (A \cup B) = (C \times A) \cup (C \times B)$$

puis que, si A et B sont disjoints, il en est de même de C × A et C × B.

5. Démontrer que, quel que soit A, on a

$$A \times \varnothing = \varnothing \times A \times \varnothing.$$

6. Démontrer que, quels que soient A et B, on a

$$(A \times B = \varnothing) \iff (A = \varnothing \quad \text{ou} \quad B = \varnothing).$$

En appliquant les résultats de ces exercices aux représentants respectifs A, B, C des cardinaux quelconques α, β, γ on obtient les résultats suivants :

Théorème 3.

Quels que soient les cardinaux α, β, γ on a

1. $(\alpha\beta)\,\gamma = \alpha(\beta\gamma)$
2. $1.\alpha = \alpha.1 = \alpha$
3. $\alpha\beta = \beta\alpha$
4. $\gamma(\alpha + \beta) = \gamma\alpha + \gamma\beta$
5. $0.\alpha = \alpha.0 = 0$
6. $(\alpha\beta = 0) \iff (\alpha = 0 \text{ ou } \beta = 0)$.

Nous dirons que la multiplication des cardinaux est *associative* et *commutative* (propriétés 1 et 3); qu'elle admet 1 pour *élément neutre* (propriété 2) et qu'elle est *distributive* par rapport à l'addition des cardinaux (propriété 4).

EXERCICE

6. Démontrer que quel que soit le cardinal α on a $\alpha + \alpha = 2\,\alpha$.
(Utiliser les propriétés 2 et 4 ci-dessus et l'exercice 1 du § B.4.)

Quels que soient les cardinaux α, β, γ il est évident que si $\alpha = \beta$ alors $\alpha\gamma = \beta\gamma$. En revanche si $\alpha\gamma = \beta\gamma$ on ne peut conclure $\alpha = \beta$: c'est évident si $\gamma = 0$, dans ce cas (propriété 5) α et β sont quelconques; mais même si $\gamma \neq 0$ on ne peut conclure comme le montre l'exercice suivant.

EXERCICE

7. Supposons connu l'ensemble $\mathbb{N}$ des entiers naturels, désignons son cardinal par ν. Démontrer que $2.\nu = 1.\nu$. (Utiliser l'exercice 2 du § B.4 et l'exercice 6 ci-dessus).

Un autre contre-exemple résulte de l'exercice n° 1.64, fin du chapitre 1, où on démontre que $\mathbb{N} \times \mathbb{N}$ est équipotent à $\mathbb{N}$. Si $\nu = \text{card}\,\mathbb{N}$ on a $\nu.\nu = \nu$ et $\nu \neq 1$.

B. 6 ORDRE SUR LA CLASSE DES CARDINAUX

a) Introduction.

Reprenons l'exemple des ensembles S et P du § B.3 a). Pour savoir si $s \leqslant p$ nous pouvons procéder de deux matières :

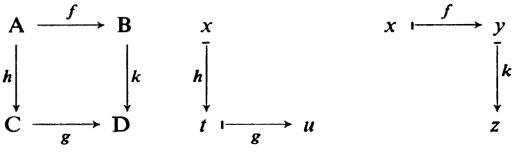
1. En « comptant » le « nombre d'éléments » de S et ceux de P.
2. En essayant de faire asseoir chaque personne sur un siège : on aura $s \leqslant p$ si et seulement si tous les sièges sont occupés (on aura $s = p$ si personne ne reste debout et $s < p$ s'il reste au moins une personne debout).

Le deuxième procédé est seul facilement généralisable aux ensembles « infinis »; il consiste, en effet, à essayer de construire une injection de S dans P.

b) Relation d'ordre entre les cardinaux α et β.

Soit A et B des ensembles représentants respectifs des cardinaux α et β, nous sommes tentés de dire que $\alpha \leqslant \beta$ si et seulement s'il existe une injection de A dans B. Ceci ne sera correct (cf. § B.3 e) que, si, A′ et B′ étant deux autres représentants de α et β, il existe aussi une injection de A′ sur B′. Nous allons montrer que ce résultat est exact.

Donnons d'abord une définition. Considérons le diagramme suivant définissant des applications (remarquez bien le sens des flèches).



Grâce à ce diagramme nous pouvons définir deux applications de A dans D

$$g \circ h : A \longrightarrow D \qquad k \circ f : A \longrightarrow D$$
$$x \longmapsto u \qquad x \longmapsto z.$$

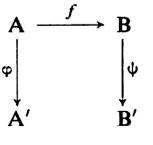
Nous dirons que le **diagramme est commutatif** si et seulement si, quel que soit x de A, on a $z = u$ c'est-à-dire

$$(\forall\, x \in A) \qquad (g \circ h)(x) = (k \circ f)(x),$$

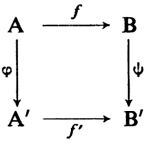
ou encore

$$g \circ h = k \circ f.$$

Cette définition étant posée, considérons le diagramme



où φ et ψ sont des *bijections* et f une *injection*. Nous nous proposons de montrer qu'il existe une injection $f' : A' \longrightarrow B'$.
Supposons qu'il existe une application $f' : A' \longrightarrow B'$ telle que le diagramme



soit commutatif, on aura

(1) $$f' \circ \varphi = \psi \circ f.$$

Or φ est une bijection, en composant les deux membres de l'égalité (1) à droite par φ^{-1} on obtient

(1') $$f' = \psi \circ f \circ \varphi^{-1}.$$

Considérons a priori cette application

$$A' \xrightarrow{\varphi^{-1}} A \xrightarrow{f} B \xrightarrow{\psi} B' \qquad (f')$$

C'est une application de A' dans B', montrons qu'elle vérifie (1), en effet

$$(\psi \circ f \circ \varphi^{-1}) \circ \varphi = \psi \circ f.$$

D'autre part f est injective; il en est de même de ψ et φ^{-1} qui sont des bijections donc, comme vous le savez, $f' = \psi \circ f \circ \varphi^{-1}$ est une *injection*.
Donc il existe une injection f de A dans B, il existe une injection f' de A' dans B'; autrement dit, quels que soient les cardinaux α et β de représentants respectifs A et B la relation « il existe une injection de A dans B » est indépendante des représentants choisis.

Nous définissons ainsi une relation entre cardinaux, c'est une *relation définie sur la classe de tous les cardinaux*.

Propriétés de cette relation.

Quel que soit le cardinal α de représentant A, l'application Id_A est une injection de A dans A (elle est bijective); nous dirons que la relation considérée est *réflexive*.
Quels que soient les cardinaux α, β, γ de représentants respectifs A, B, C, s'il existe une injection f de A dans B et une injection g de B dans C, alors il existe une injection de A dans C à savoir $g \circ f$, car, comme vous le savez, la composée de deux injections est une injection. Nous dirons que la relation considérée est *transitive*.

Nous admettrons le résultat suivant connu sous le nom de théorème de BERNSTEIN :

Quels que soient les ensembles A *et* B *s'il existe une injection de* A *dans* B *et une injection de* B *dans* A, *alors* A *et* B *sont équipotents.*
Nous dirons que la relation considérée est *antisymétrique*.

Nous sommes tout naturellement amenés à dire que la relation considérée est une *relation d'ordre définie sur la classe de tous les cardinaux*.

Théorème et définition 4.

Quels que soient les cardinaux α et β de représentants respectifs A et B la relation

« il existe une injection de A dans B »

est indépendante des représentants choisis.
Cette relation est réflexive, antisymétrique et transitive. Nous l'énoncerons : le cardinal α est **inférieur** au cardinal β et nous la noterons

$$\alpha \leqslant \beta.$$

Nous admettrons le résultat suivant :

Quels que soient les ensembles A et B, il existe une injection de A dans B ou une injection de B dans A.

Il en résulte que quels que soient les cardinaux α et β l'énoncé

$$\alpha \leqslant \beta \quad \text{ou} \quad \beta \leqslant \alpha$$

est toujours vrai. Nous sommes amenés à dire que la *relation* $\alpha \leqslant \beta$ *entre les cardinaux* α et β est une **relation d'ordre total.**
La relation

$$\alpha \leqslant \beta \quad \text{et} \quad \alpha \neq \beta$$

s'énonce : le cardinal α est **strictement inférieur** au cardinal β et se note $\alpha < \beta$.
Si A et B sont des représentants respectifs de α et β, la relation $\alpha < \beta$ signifie donc : il y a des injections de A dans B et aucune de ces injections n'est bijective.

EXERCICES

1. Donner la signification de $\alpha \geqslant \beta$, de $\alpha > \beta$.
2. Démontrer que la relation $\alpha < \beta$ est transitive.
3. Démontrer que $0 < 1$, que $1 < 2$.

c) Applications.

Application 1. Un exemple trivial.

Soit A et B deux ensembles tels que $A \subset B$; considérons l'application f de A dans B définie par

$$(\forall x \in A) \qquad f(x) = x$$

c'est manifestement une *injection*.
Rappelons que f est appelée *injection canonique* de A, partie de B, dans B.

Théorème 4.

Quels que soient les ensembles A et B on a

$$(A \subset B) \Longrightarrow (\text{card } A \leqslant \text{card } B).$$

Pour tout ensemble A on a $\varnothing \subset A$ donc :

Corollaire 1.

Quel que soit le cardinal α on a

$$0 \leqslant \alpha.$$

Pour tout ensemble non vide, il existe $\{a\} \subset A$ donc :

Corollaire 2.

Quel que soit le cardinal $\alpha \neq 0$ on a

$$1 \leqslant \alpha.$$

REMARQUES

1. Si $A \subset B$ et $A \neq B$, on ne peut affirmer que (card A < card B); par exemple, si nous supposons connu l'ensemble $\mathbb{N}$ des « entiers naturels », $2\,\mathbb{N}$ est l'ensemble des « entiers pairs » et nous avons $2\,\mathbb{N} \subset \mathbb{N}$ et $2\,\mathbb{N} \neq \mathbb{N}$ mais (cf. B.3 ex. 1) card $(2\,\mathbb{N})$ = card $(\mathbb{N})$.
2. Soit E et F des représentants respectifs des cardinaux $\alpha \leqslant \beta$ vérifiant α et β; il existe donc une injection f de E dans F; considérons l'application g de E dans f (E) telle que

   $$(\forall x \in E) \qquad g(x) = f(x);$$

   l'application g est d'après sa définition surjective; de plus elle est injective, car f l'est; g est donc bijective et E et f (E) sont équipotents.
   Or f (E) $\subset$ F; donc A = f (E) et B = F sont des représentants de α et β vérifiant $A \subset B$.
   Concluons :

Si $\alpha \leqslant \beta$ on peut toujours trouver un représentant A de α et un représentant B de β tel que $A \subset B$.

Application 2. Un exemple remarquable.

Soit E un ensemble quelconque et $\mathfrak{T}$ (E) l'ensemble de ses parties. Quel que soit x de E, $\{x\}$ est un élément de $\mathfrak{T}$ (E); considérons l'application

$$\begin{aligned} i : E &\longmapsto \mathfrak{T}(E) \\ x &\longmapsto \{x\} \end{aligned}$$

cette application est manifestement *injective*, donc

$$\text{card } E \leqslant \text{card } \mathfrak{T}(E).$$

Nous allons démontrer que card E $\neq$ card $\mathfrak{T}$ (E); c'est-à-dire qu'il n'existe pas de bijection de E sur $\mathfrak{T}$ (E).

Supposons qu'il existe une bijection f de E sur $\mathfrak{T}(E)$. A tout élément x de E est associée $f(x)$ partie de E; on aura donc ou bien $x \in f(x)$, ou bien $x \notin f(x)$; désignons par A la partie suivante de E :

$$A = \{x \in E \mid x \notin f(x)\}.$$

L'application f étant bijective, il existe un élément unique a de E tel que $f(a) = A$. Nous allons montrer que cet énoncé est faux. En effet si a existe, on a soit $a \in f(a) = A$ soit $a \notin A$. Or par définition de A les deux énoncés $a \in A$ et $a \notin A$ sont faux tous les deux; donc a n'existe pas et notre hypothèse est fausse. Concluons :

Théorème 5.

Quel que soit l'ensemble E

$$\text{card } E < \text{card } \mathfrak{T}(E).$$

REMARQUE

3. Ce théorème va nous montrer que la classe $\mathfrak{U}$ de tous les ensembles n'est pas un ensemble. En effet si $\mathfrak{U}$ était un ensemble, on pourrait lui appliquer tous les résultats que nous connaissons sur les ensembles. En particulier on aurait $\text{card } \mathfrak{U} < \text{card } \mathfrak{T}(\mathfrak{U})$ (théorème 5). D'autre part toutes les parties de $\mathfrak{U}$ seraient des ensembles, donc des éléments de $\mathfrak{U}$ et par conséquent $\mathfrak{T}(\mathfrak{U})$ serait une partie de $\mathfrak{U}$, d'où $\text{card } \mathfrak{T}(\mathfrak{U}) \leqslant \text{card } \mathfrak{U}$ (théorème 4). De la transitivité de la relation d'ordre on déduirait car $\mathfrak{U} < \text{card } \mathfrak{U}$, énoncé faux; donc notre hypothèse est fausse et par conséquent *la classe $\mathfrak{U}$ de tous les ensembles n'est pas un ensemble.*

B. 7 PROPRIÉTÉS CONJOINTES DES OPÉRATIONS ET DE L'ORDRE DÉFINIS SUR LA CLASSE DE TOUS LES CARDINAUX

Sur la classe de tous les cardinaux nous avons défini une addition (§ B.4) une multiplication (§ B.5) et un ordre total (§ B.6). Nous allons voir qu'il y a des relations entre addition et ordre et entre multiplication et ordre.

a) Compatibilité de l'addition et de l'ordre.

Quels que soient les cardinaux α et β vérifiant $\alpha \leqslant \beta$ nous pouvons choisir des représentants A et B tels que $A \subset B$ (cf. § B.6 c remarque 2).
Soit γ un cardinal quelconque de représentant C. En posant

$$A' = A \times \{0\} \quad , \quad B' = B \times \{0\} \quad , \quad C' = C \times \{1\}$$

nous avons (cf. § B.4 b)

$$\text{card } A' = \alpha \quad , \quad \text{card } B' = \beta \quad , \quad \text{card } C' = \gamma$$

et

$$A' \cap C' = B' \cap C' = \varnothing.$$

De plus on voit que $A' \subset B'$ (car $A \subset B$); on a donc

$$(A' \cup C') \subset (B' \cup C');$$

d'où (cf. § B.6, théorème 4)

$$\text{card } (A' \cup C') \leqslant \text{card } (B' \cup C')$$

c'est-à-dire

$$\alpha + \gamma \leqslant \beta + \gamma.$$

Théorème 6.

Quels que soient les cardinaux α, β, γ on a

$$(\alpha \leqslant \beta) \Longrightarrow (\alpha + \gamma \leqslant \beta + \gamma).$$

Supposons $\alpha \leqslant \beta$, nous pouvons choisir des représentants tels que $A \subset B$; posons

$$\gamma = \text{card } \complement_B A;$$

on a

$$A \cup \complement_B A = B \quad \text{et} \quad A \cap \complement_B A = \varnothing$$

d'où

$$\beta = \alpha + \gamma.$$

Réciproquement supposons que les cardinaux α et β soient tels qu'il existe un cardinal γ vérifiant $\beta = \alpha + \gamma$. De la relation $0 \leqslant \gamma$ (cf. § B.6 c) on déduit grâce au théorème 6 :

$$0 + \alpha \leqslant \alpha + \gamma = \beta;$$

d'où $\alpha \leqslant \beta$; nous pouvons énoncer :

Corollaire 1.

Quels que soient les cardinaux α et β, les propriétés suivantes sont équivalentes :

1. $\alpha \leqslant \beta$
2. Il existe un cardinal γ tel que $\beta = \alpha + \gamma$.

Soit α un cardinal non nul; on a (cf. § B.6 c, corollaire 2) $1 \leqslant \alpha$; il existe donc un cardinal β tel que $\alpha = \beta + 1$.

Corollaire 2.

Pour tout cardinal α non nul il existe un cardinal β tel que $\alpha = \beta + 1$.

b) Compatibilité de la multiplication et de l'ordre.

Quels que soient les cardinaux α et β vérifiant $\alpha \leqslant \beta$, nous pouvons choisir des représentants A et B tels que $A \subset B$ (cf. § B.6 c, remarque 2). Soit γ un cardinal quelconque de représentant C, on aura

$$(A \times C) \subset (B \times C),$$

d'où, grâce au théorème 4,

$$\text{card}\,(A \times C) \leqslant \text{card}\,(B \times C),$$

c'est-à-dire

$$\alpha\gamma \leqslant \beta\gamma.$$

Théorème 7.

Quels que soient les cardinaux α, β, γ on a

$$(\alpha \leqslant \beta) \Longrightarrow (\alpha\gamma \leqslant \beta\gamma).$$

B. 8 ENSEMBLES ET CARDINAUX FINIS; ENSEMBLES ET CARDINAUX INFINIS

a) Introduction.

Considérons un ensemble « fini » par exemple $E = \{a, b, c\}$ ayant « trois « éléments. Nous pouvons montrer facilement que toute application de E dans une de ses parties propres est non bijective. Ce qui revient à dire qu'il n'existe pas de partie propre de E équipotente à E. En revanche considérons l'ensemble $\mathbb{N}$ des « entiers naturels », l'ensemble $2\,\mathbb{N}$ des « entiers naturels pairs » est une partie propre de $\mathbb{N}$; or à l'exercice 1 du § B.3 nous avons montré que $\mathbb{N}$ et $2\,\mathbb{N}$ sont équipotents.
Donc pour $\mathbb{N}$ qui est un ensemble « infini », au sens intuitif du terme, il existe une partie propre de $\mathbb{N}$ équipotente à $\mathbb{N}$. Ceci nous amène à donner les définitions suivantes des ensembles infinis et des ensembles finis.

b) Ensembles et cardinaux infinis.

Définition 5.

Un ensemble E est infini si et seulement si E possède la propriété suivante : il existe une partie propre de E équipotente à E.

Soit E un ensemble possédant une partie propre A équipotente à E. On a

$$A \subset E \quad \text{et} \quad A \neq E.$$

Posons $\alpha = \text{card}\,E = \text{card}\,A.$

Il existe a de E n'appartenant pas à A; on a donc

$$A \cap \{a\} = \varnothing \quad \text{et} \quad A \subset (A \cup \{a\}) \subset E;$$

on en déduit card $A \cup \{a\} = \alpha + 1$ et (cf. § B.6, théorème 4)

$$\alpha \leqslant \alpha + 1 \leqslant \alpha;$$

d'où

$$\alpha + 1 = \alpha.$$

Réciproquement soit un ensemble E de cardinal α vérifiant $\alpha + 1 = \alpha$.
On sait que $\alpha \geqslant 0$, donc $\alpha + 1 \geqslant 0 + 1 = 1$ et par conséquent $\alpha \geqslant 1$; tout ensemble E de cardinal α tel que $\alpha + 1 = \alpha$ est donc non vide. Soit $a \in E$, posons

$$E' = E - \{a\} \quad , \quad \text{card } E' = \alpha';$$

nous avons $E = E' \cup \{a\}$; comme $a \notin E'$, les ensembles E' et $\{a\}$ sont disjoints, donc on a

$$\alpha = \text{card } E = \text{card } (E' \cup \{a\}) = \alpha' + 1.$$

On en déduit $\alpha + 1 = \alpha' + 1$ d'où (§ B.4, théorème 2) $\alpha = \alpha'$.
L'ensemble E possède donc une partie propre — à savoir E' — équipotente à E. Concluons :

Théorème 8.

Pour tout ensemble E les deux propriétés suivantes sont équivalentes :
1. Il existe une partie propre de E équipotente à E.
2. (card E) + 1 = card E.

Définition 6.

On dit qu'un cardinal α est **infini** si et seulement si $\alpha + 1 = \alpha$.

Le théorème 8 montre qu'un cardinal est infini si et seulement si un de ses représentants est infini : tous ses représentants sont alors infinis.

c) Ensembles et cardinaux finis.

Définition 7.

Tout ensemble qui n'est pas infini est appelé **ensemble fini.**
Tout cardinal qui n'est pas infini est appelé **cardinal fini.**

Pour tout ensemble fini, il n'existe donc pas de partie propre équipotente à E.
Pour tout cardinal α fini, on a donc

$$\alpha + 1 \neq \alpha.$$

La relation $0 \leqslant 1$ entraîne, pour tout cardinal α, $\alpha \leqslant \alpha + 1$; donc *un cardinal est fini si et seulement si* $\alpha < \alpha + 1$.
On peut donc caractériser un ensemble E infini (resp. fini) de cardinal α de deux manières :

1. Existence (resp. non existence) d'une partie propre équipotente à E.
2. $\alpha + 1 = \alpha$ (resp. $\alpha + 1 \neq \alpha$).

La première est plus intuitive, la deuxième est souvent plus pratique dans les applications.
Par exemple comme $0 \neq 1$, *0 est un cardinal fini* et *le vide est un ensemble fini.*
De même soit α un cardinal quelconque, posons $\beta = \alpha + 1$; les propriétés suivantes sont équivalentes :

1. α est infini.
2. $\alpha = \beta$.
3. $\alpha + 1 = \beta + 1$ (cf. § B.4, théorème 2).
4. $\alpha + 1$ est infini.

Donc α est infini et seulement si $\alpha + 1$ est infini; il en résulte, par négation, que α est fini si et seulement si $\alpha + 1$ est fini. Concluons :

Théorème 9.

Un cardinal α est fini (resp. infini) si et seulement si $\alpha + 1$ est fini (resp. infini).

Soit α un cardinal fini et β un cardinal tel que $\beta \leqslant \alpha$. Il existe donc un cardinal γ tel que $\alpha = \beta + \gamma$ (cf. § B.7, cor. 1 du th. 6) et on a

$$(\beta + 1) + \gamma = (\beta + \gamma) + 1 = \alpha + 1;$$

or α est fini donc $\alpha \neq \alpha + 1$ (th. 9), on en déduit

$$(\beta + 1) + \gamma \neq \beta + \gamma$$

donc $\beta + 1 \neq \beta$ (sinon on aurait $(\beta + 1) + \gamma = \beta + \gamma$) et par conséquent β est fini.

Corollaire 1.

Tout cardinal inférieur à un cardinal fini est fini.

On en déduit immédiatement

Corollaire 2.

Toute partie d'un ensemble fini est finie.

B. 9 ENSEMBLE $\mathbb{N}$ DES ENTIERS NATURELS

a) Ensemble totalement ordonné des entiers naturels.

Nous **admettrons** le résultat suivant : **Il existe un ensemble, noté $\mathbb{N}$, dont les éléments sont tous les cardinaux finis.**

Définition 8.

Les éléments de $\mathbb{N}$ sont appelés **nombres entiers naturels** ou plus simplement **entiers naturels.**

Dans l'annexe B n'étudiant que les entiers naturels, il nous arrivera de dire entier pour entier naturel.
Par exemple $0, 1, 1 + 1 = 2$ sont des entiers naturels. D'après les définitions données au paragraphe précédent, tout ensemble fini E a pour cardinal un entier naturel; si $E = \varnothing$, c'est 0, si E **fini est non vide,** son cardinal entier naturel est appelé **nombre d'éléments de E.**
La relation d'ordre entre les cardinaux devient, pour les entiers naturels une **relation d'ordre définie sur l'ensemble** $\mathbb{N}$. Nous supposerons que $\mathbb{N}$ est toujours muni de cette relation d'ordre.
Rappelons que cet **ordre est total.** Il est appelé **ordre naturel** défini sur $\mathbb{N}$.
Nous poserons

$$\mathbb{N}^* = \mathbb{N} - \{0\} = \{x \in \mathbb{N} \mid 0 < x\}.$$

b) Propriété fondamentale et principe de récurrence.

Nous **admettrons** le résultat suivant dont la démonstration est assez délicate :

Théorème 10.

Toute partie non vide de $\mathbb{N}$ a un plus petit élément.

Soit X une partie de $\mathbb{N}$ possédant les propriétés suivantes :
1. $0 \in X$.
2. $(\forall x \in X) \quad x + 1 \in X$.

Rappelons que si x est un entier, c'est-à-dire un cardinal fini, il en est de même de $x + 1$ (th. 9).
Soit Y le complémentaire de X dans $\mathbb{N}$. Si Y est vide, nous avons $X = \mathbb{N}$.
Supposons $Y \neq \varnothing$, Y a donc un plus petit élément a (th. 10); comme $0 \in X$ on a $a > 0$; il existe donc un cardinal β tel que $a = \beta + 1$ (cf. B.7, cor. 2 du th. 6); or $\beta + 1$ est fini, donc β également (cf. B.8, th. 9); il existe donc un entier naturel $b = \beta$ tel que $a = b + 1$; par conséquent $b < a$; il en résulte que b n'appartient pas à Y (a est le plus petit élément de Y), donc $b \in X$; d'après l'hypothèse 2 on a $b + 1 = a \in X$, ce qui est impossible puisque $a \in Y$. Donc l'hypothèse $Y \neq \varnothing$ est fausse; par conséquent on a $Y = \varnothing$, d'où $X = \mathbb{N}$.

Théorème 11.

Toute partie X de $\mathbb{N}$ possédant les deux propriétés suivantes :

1. $0 \in X$
2. $(\forall x \in X) \quad x + 1 \in X$

est égale à $\mathbb{N}$.

Rappelons que l'on appelle *propriété définie sur un ensemble* E, *ou propriété ayant un sens sur* E, une propriété possédée par certains éléments de E et non possédée par tous les autres éléments de E.

Soit $\mathcal{P}$ une propriété définie sur $\mathbb{N}$ telle que

1. $\mathcal{P}(0)$ est un énoncé vrai.
2. $(\forall x \in \mathbb{N}) \quad \mathcal{P}(x) \Longrightarrow \mathcal{P}(x+1)$.

Posons $X = \{x \in \mathbb{N} \mid \mathcal{P}(x)\}$

nous avons $0 \in X$

et, dès que $\mathcal{P}(x)$ est vrai, c'est-à-dire dès que $x \in X$, alors $\mathcal{P}(x+1)$ est vrai, c'est-à-dire $x + 1 \in X$; d'où :

$$(\forall x \in X) \quad x + 1 \in X$$

donc (théorème 11) $X = \mathbb{N}$, c'est-à-dire

$$(\forall x \in \mathbb{N}) \quad \mathcal{P}(x).$$

D'où le résultat suivant appelé **principe du raisonnement par récurrence :**

Corollaire.

Si $\mathcal{P}$ est une propriété définie sur $\mathbb{N}$ telle que

1. $\mathcal{P}(0)$ est vraie.
2. $(\forall x \in \mathbb{N}) \quad \mathcal{P}(x) \Longrightarrow \mathcal{P}(x+1)$

alors $\mathcal{P}(x)$ est vraie pour tout entier naturel x.

Le premier membre, $\mathcal{P}(x)$, de l'implication 2 porte le nom d'*hypothèse de récurrence*.

c) Addition et multiplication des entiers naturels.

Soient a et b deux entiers. Nous allons montrer par récurrence que $a + b$ est un entier. Nous raisonnons par récurrence sur b, en supposant que a est un entier quelconque fixé.

La propriété à démontrer est vraie pour $b = 0$ car $a + 0 = a$.

Supposons-la vraie pour b; donc nous supposons que $a + b$ est un cardinal fini (hypothèse de récurrence). Par conséquent (th. 9) $(a + b) + 1$ est aussi un cardinal fini; or on a (associativité de la somme des cardinaux)

$$(a + b) + 1 = a + (b + 1);$$

donc $a + (b + 1)$ est un entier et la propriété est vraie pour $b + 1$. Elle est donc vraie quel que soit b.

Montrons maintenant que ab est un entier. Nous raisonnons par récurrence sur b, en supposant que a est un entier quelconque fixé.

La propriété à démontrer est vraie pour $b = 0$ car $a.0 = 0$ est un entier.

Supposons-la vraie pour b; donc nous supposons que ab est un cardinal fini (hypothèse de récurrence). On a (distributivité de la multiplication des cardinaux par rapport à leur addition)

$$a(b + 1) = ab + a.1 = ab + a;$$

or ab et a sont des entiers, donc leur somme $ab + a$ est aussi un entier. Donc $a(b + 1)$ est un entier et par conséquent la propriété est donc vraie quel que soit b.

Théorème 12.

La somme et le produit de deux entiers naturels est un entier naturel

EXERCICE

Soient deux cardinaux α et β ayant pour somme un entier n, démontrer que α et β sont des entiers. (Utiliser § B.7 cor. 1 du th. 6 et § B.8 cor. du th. 9.)

Naturellement l'addition et la multiplication des entiers naturels possèdent toutes les propriétés de ces deux opérations effectuées sur des cardinaux quelconques : *associativité*, *commutativité*, *éléments neutres* 0 et 1, *distributivité* de la multiplication par rapport à l'addition.
Mais de plus l'addition et la multiplication dans $\mathbb{N}$ possèdent des propriétés que ne possèdent pas l'addition et la multiplication dans la classe de tous les cardinaux.

d) Égalité et opérations dans $\mathbb{N}$.

Quels que soient les entiers naturels a, b, x nous allons montrer que

(1) $$(a + x = b + x) \Longrightarrow (a = b)$$

c'est-à-dire que tout entier naturel est *régulier* pour l'addition (cf. § 1.1).
Prenons deux entiers naturels a et b quelconques. L'implication (1) est vraie pour $x = 0$.
Supposons-la vraie pour x, hypothèse de récurrence. La relation

$$a + (x + 1) = b + (x + 1)$$

peut s'écrire (associativité de l'addition des cardinaux)

$$(a + x) + 1 = (b + x) + 1;$$

d'où d'après le théorème 2 du § B.4 on a $a + x = b + x$; donc d'après l'hypothèse de récurrence on a $a = b$. Donc si l'implication (1) est vraie pour x, alors elle est vraie pour $x + 1$. Étant vraie pour $x = 0$, elle est vraie pour tout entier naturel.
Démontrons maintenant que, *quels que soient les entiers naturels* a, b *et quel que soit l'entier naturel* **non nul** x on a

$$(ax = bx) \Longrightarrow (a = b),$$

c'est-à-dire que tout entier naturel *non nul* est régulier pour la multiplication dans $\mathbb{N}$.
Supposons vérifiée l'égalité $ax = bx$. L'ordre naturel défini sur $\mathbb{N}$ étant total (cf. § B.9 a), on a $a \leqslant b$ ou $b \leqslant a$; nous ne nuirons pas à la généralité de la démonstration en supposant $a \leqslant b$. Il existe donc un cardinal γ tel que $b = a + \gamma$ et $\gamma \leqslant b$ (cf. § B.7 a, cor. 1 du th. 6); b étant un entier, donc un cardinal fini, il en est de même de $\gamma \leqslant b$ (cf. § B.8 c, cor. 1 du th. 9). Il existe donc un entier naturel c tel que $b = a + c$. Nous avons donc

$$ax = (a + c)\, x$$

qui s'écrit, d'après la distributivité,

$$ax = ax + cx;$$

d'où, tout entier naturel étant régulier pour l'addition,

$$0 = cx.$$

Or $x \neq 0$ donc (cf. § B.5, propriété 6 du th. 3) $c = 0$ et par conséquent $a = b$.
Concluons :

Théorème 13.

1. Tout entier naturel est régulier pour l'addition dans $\mathbb{N}$.
2. Tout entier naturel **non nul** est régulier pour la multiplication dans $\mathbb{N}$.

Rappelons que ces propriétés ne sont pas vraies pour les cardinaux quelconques (cf. § B.4 c et B.5 c). Nous avons cependant le résultat suivant :

EXERCICE

2. Quels que soient les cardinaux α et β et quel que soit l'entier naturel x on a

$$(\alpha + x = \beta + x) \Longrightarrow (\alpha = \beta).$$

(Faire un raisonnement par récurrence sur x et utiliser le théorème 2 du § B.4 c.)

B. 10 ORDRE NATUREL ET OPÉRATIONS DÉFINIS SUR $\mathbb{N}$. APPLICATIONS

Nous considérons dans ce paragraphe $(\mathbb{N}, +, \times, \leqslant)$ c'est-à-dire l'ensemble $\mathbb{N}$ des entiers naturels muni à la fois de l'addition, de la multiplication des entiers naturels et de l'ordre naturel défini sur $\mathbb{N}$.

a) Compatibilité de l'ordre naturel et des opérations définis sur $\mathbb{N}$.

Les propriétés suivantes étant vraies pour des cardinaux quelconques (cf. § B.7 a et b), quels que soient a, b, x de $\mathbb{N}$, on a

$$(a \leqslant b) \Longrightarrow (a + x \leqslant b + x),$$
$$(a \leqslant b) \Longrightarrow (ax \leqslant bx),$$

propriétés que l'on exprime en disant que l'ordre naturel défini sur $\mathbb{N}$ est compatible avec l'addition et la multiplication définies sur $\mathbb{N}$.

Supposons que l'on ait $a < b$; on a donc $a \leqslant b$ et $a + x \leqslant b + x$ quel que soit x; par conséquent nous avons soit $a + x < b + x$, soit $a + x = b + x$; dans cette deuxième éventualité on aurait $a = b$, tout entier naturel étant régulier pour l'addition; on a donc $a + x < b + x$.
Réciproquement si on a $a + x < b + x$, il y a, a priori trois éventualités pour a et b

$$a = b \quad , \quad a < b \quad , \quad b < a;$$

la première et la troisième impliquent respectivement $a + x = b + x$ et $b + x < a + x$, résultats tous deux contraires à notre hypothèse; on a donc $a < b$.
Par conséquent quels que soient les entiers a, b, x

$$(a < b) \Longleftrightarrow (a + x < b + x).$$

Supposons que l'on ait $a < b$ et $0 < x$; on a donc $a \leqslant b$ et $ax \leqslant bx$, quel que soit x; par conséquent nous avons soit $ax < bx$, soit $ax = bx$; dans cette deuxième éventualité on aurait $a = b$, car $x \neq 0$ est régulier pour la multiplication; on a donc $a + x < b + x$.
Réciproquement si on a $ax < bx$ et $0 < x$, il y a, a priori, trois éventualités pour a et b

$$a = b \quad , \quad a < b \quad , \quad b < a;$$

la première et la troisième impliquent respectivement $ax = bx$, $bx < ax$ (car $0 < x$), résultats tous deux contraires à notre hypothèse; on a donc $a < b$.
Par conséquent quels que soient a, b de $\mathbb{N}$ et x de $\mathbb{N}^*$ on a

$$(a < b) \Longleftrightarrow (ax < bx).$$

Théorème 14.

1. L'ordre naturel défini sur $\mathbb{N}$ est compatible avec l'addition et la multiplication des entiers naturels.
2. Quels que soient a, b, x de $\mathbb{N}$ on a
$$(a < b) \Longleftrightarrow (a + x < b + x).$$
3. Quels que soient a, b de $\mathbb{N}$ et x de $\mathbb{N}^*$ on a
$$(a < b) \Longleftrightarrow (ax < bx).$$

Rappelons que les propriétés 2 et 3 ne sont pas vérifiées par les cardinaux quelconques (cf. § B.7).

b) Différence et quotient de deux entiers naturels.

Soient deux entiers naturels a et b tels que $a \leqslant b$; il existe un cardinal γ tel que $b = a + \gamma$ (cf. § B.7, cor. 1 du th. 6) et $\gamma \leqslant b$ donc γ est égal à un cardinal fini c (cf. § B.8, cor. 1 du th. 9). Il existe donc c de $\mathbb{N}$ tel que $b = a + c$; c est unique car $b = a + c = a + c'$ implique $c = c'$. Cet entier unique se note $b - a$; il est appelé *différence* de b et de a; notons que cette différence n'est définie que pour $a \leqslant b$.

On dit que l'entier naturel a est divisible par l'entier naturel **non nul** b si et seulement s'il existe un entier naturel d tel que

$$a = bd.$$

Si d existe, il est unique; en effet, $a = bd = bd'$, avec $b \neq 0$, implique $d = d'$. Cet entier d est noté $\frac{a}{b}$; il est appelé quotient de a par b; ce quotient n'est défini que si a est divisible par b.

Théorème 15.

1. Pour tout couple $(a, b) \in \mathbb{N} \times \mathbb{N}$ vérifiant $a \leqslant b$, il existe un entier naturel unique c, noté $b - a$, tel que $b = a + c$.
2. Pour tout couple d'entiers $(a, b) \in \mathbb{N} \times \mathbb{N}^*$, tel que a soit divisible par b, il existe un entier naturel unique d, noté $\frac{a}{b}$ tel que $a = bd$.

EXERCICES

1. Démontrer que, quel que soit x de $\mathbb{N}$, si $b - a$ existe, alors $(b + x) - (a + x)$ existe et $b - a = (b + x) - (a + x)$.
2. Démontrer que la relation définie sur $\mathbb{N}^*$ par « b divise a » est une relation d'ordre. Cet ordre est-il total?
3. Démontrer que, quel que soit x de $\mathbb{N}^*$, si $\frac{a}{b}$ existe, alors $\frac{ax}{bx}$ existe et $\frac{a}{b} = \frac{ax}{bx}$.

c) Application 1.

On a vu au § B.6 c que pour tout cardinal α on a $\alpha \geqslant 0$ et pour tout cardinal $\alpha \neq 0$ on a $\alpha \geqslant 1$. Soit a un *entier naturel non nul*, on a donc $a > 0$, d'où $a \geqslant 1$; réciproquement si $a \geqslant 1$, $a = 0$ est impossible puisque $0 < 1$ on a donc $a > 0$. Concluons :

Quel que soit a de $\mathbb{N}$

$$(a > 0) \iff (a \geqslant 1).$$

On peut énoncer ceci en disant qu'il n'y a aucun entier naturel strictement compris entre 0 et 1. D'autre part, d'après le théorème 14, quels que soient a et x de $\mathbb{N}$ on a

$$(0 < x < 1) \iff (a < x + a < a + 1);$$

on en déduit facilement

Quel que soit l'entier naturel a, il n'existe aucun entier naturel strictement compris entre a et $a + 1$.

Intuitivement cela signifie que si e n'appartient pas à l'ensemble fini A, il n'existe aucun ensemble strictement compris entre A et A $\cup$ $\{e\}$.

d) Application 2.

Soit x un entier naturel quelconque, alors $x + 1 \geqslant 1$ donc $x + 1 > 0$. Considérons l'application

$$f : \mathbb{N} \longrightarrow \mathbb{N}^*$$
$$x \longmapsto x + 1.$$

Quel que soit y de $\mathbb{N}^*$ on a $y \geqslant 1$; donc (th. 15) l'équation $f(x) = y$, c'est-à-dire $x + 1 = y$ a une solution unique dans $\mathbb{N}$ à savoir $x = y - 1$. Il en résulte que f est une bijection; donc $\mathbb{N}$ est équipotent à $\mathbb{N}^*$ partie stricte de $\mathbb{N}$, d'où (cf. § B.8, définition 5)

Théorème 16.

$\mathbb{N}$ est un ensemble infini.

B. 11 INTERVALLES DE $\mathbb{N}$. PARTIES MAJORÉES DE $\mathbb{N}$.

a) Définition des intervalles de $\mathbb{N}$.

Quels que soient les entiers naturels a et b vérifiant $a \leqslant b$, on appelle **intervalle** de $\mathbb{N}$ l'un quelconque des sous-ensembles de $\mathbb{N}$ suivants :

$$\begin{aligned}
[a, b] &= \{x \in \mathbb{N} \mid a \leqslant x \leqslant b\} \\
]a, b[&= \{x \in \mathbb{N} \mid a < x < b\} \\
[a, b[&= \{x \in \mathbb{N} \mid a \leqslant x < b\} \\
]a, b] &= \{x \in \mathbb{N} \mid a < x \leqslant b\} \\
[a, +\infty[&= \{x \in \mathbb{N} \mid a \leqslant x\} \\
]a, +\infty[&= \{x \in \mathbb{N} \mid a < x\}.
\end{aligned}$$

Remarquons que $\mathbb{N} = [0, +\infty[$.
Avec ces notations le résultat obtenu au § B.10 (application 1) s'énonce

$$(\forall\, a \in \mathbb{N}) \qquad]a, a+1[= \varnothing$$

Si $a \neq 0$ on a $a \geqslant 1$, donc $a - 1$ existe et on a

$$(\forall\, a \in \mathbb{N}^*) \qquad]a-1, a[= \varnothing.$$

On exprime ces propriétés en disant que tout entier naturel a a un *successeur* $a + 1$ et que tout entier naturel $a \neq 0$ a un prédécesseur $a - 1$.

b) Parties majorées non vides de $\mathbb{N}$.

Rappelons que nous avons admis au § B.9 le résultat suivant (th. 10) : *Toute partie non vide de $\mathbb{N}$ a un plus petit élément*. Comme vous le savez (cf. § 1.2. c) ce plus petit élément est unique.
Ce résultat et certains de ceux que nous avons démontrés depuis cet énoncé vont nous permettre de démontrer une propriété importante des *parties non vides majorées* de $\mathbb{N}$.
Soit A une partie majorée non vide de $\mathbb{N}$; il existe donc un entier naturel m tel que, quel que soit x de A, $x \leqslant m$ (cf. § 1.2).
Considérons l'ensemble des majorants de A dans $\mathbb{N}$, cet ensemble d'entiers naturels n'est pas vide, puisque $m \in$ M ; il a donc un plus petit élément a (théorème 10) qui est, naturellement un majorant de A.
Nous allons montrer que $a \in$ A.
Si $a = 0$, on a A $\subset \{x \in \mathbb{N} \mid x \leqslant 0\} = \{0\}$, comme A n'est pas vide, A $= \{0\}$; donc, dans ce cas, $a \in$ A.
Si $a \neq 0$, on a $a \geqslant 1$ et $a - 1 \in \mathbb{N}$. Si $a \notin$ A, $a - 1$ est un majorant de A puisque $]a-1, a[$ est vide ; donc a ne serait pas le plus petit majorant de A ; notre hypothèse est donc fausse, donc $a \in$ A.
Par conséquent a, majorant de A, appartient à A c'est le plus grand élément de A (cf. § 1.2 c).
Concluons :

Théorème 17.

Toute partie non vide majorée de $\mathbb{N}$ a un plus grand élément.

c) Propriétés des intervalles de $\mathbb{N}$.

Soit I un intervalle de $\mathbb{N}$, la transitivité de l'ordre naturel montre que, *quels que soient* c et d de I, *on a* $[c, d] \subset$ I.
Cette remarque va nous permettre de ramener les intervalles non vides de $\mathbb{N}$ à deux types seulement.
Soit I un intervalle *non vide* de $\mathbb{N}$, il a donc un plus petit élément a (th. 10).
Si I non vide est *majoré*, il a aussi un plus grand élément b (th. 17) donc pour tout x de I on a $a \leqslant x \leqslant b$ donc I $\subset [a, b]$. D'autre part, a et b appartenant à I, on a $[a, b] \subset$ I ; donc I $= [a, b]$.
Si I non vide *n'est pas majoré*, il a un plus petit élément a, donc I $\subset [a, +\infty[$. De plus quel que soit y de $[a, +\infty[$ il existe x de I tel que $y \leqslant x$ (sinon I serait majorée) ; donc a et x appartenant à I, on a $[a, x] \subset$ I et par conséquent I comprend tout y de $[a, +\infty[$ donc $[a, +\infty[\subset$ I, d'où I $= [a, +\infty[$.

Concluons :

Théorème 18.

Tout intervalle *non vide* de $\mathbb{N}$ est de la forme
$[a, b]$, avec $a \leqslant b$, s'il est majoré,
$[a, +\infty[$ s'il n'est pas majoré.

Cherchons le cardinal de $[0, n]$ pour tout entier naturel n. On a card $[0, 0]$ = card $\{0\} = 1$. Supposons que l'on ait card $[0, n] = n + 1$, hypothèse de recurrence; on a

$$[0, n+1] = [0, n] \cup \{n+1\}$$

puisque $]n, n+1[$ est vide; d'autre part $[0, n]$ et $\{n+1\}$ sont disjoints; donc

$$\text{card } [0, n+1] = (n+1) + 1.$$

L'énoncé « card $[0, n] = n + 1$ » est vrai pour $n = 0$; étant vrai pour n, il l'est pour $n + 1$, il est donc vrai pour tout n.

Théorème 19.

Pour tout entier naturel n on a

$$\text{card } [0, n] = n + 1.$$

Si on a deux entiers naturels a et b tels que $a \leqslant b$, il existe $c = b - a$ tel que $b = a + c$. D'autre part, quel que soit x, de $\mathbb{N}$ on a

$$0 \leqslant x \leqslant c \iff (a \leqslant x + a \leqslant b)$$

vous en déduirez facilement que l'application

$$\begin{array}{ccc} [0, c] & \longrightarrow & [a, b] \\ x & \longmapsto & x + a \end{array}$$

est une bijection; donc $[a, b]$ est équipotent à $[0, b - a]$.

Corollaire 1.

Quels que soient les entiers naturels a et b tels que $a \leqslant b$ on a

$$\text{card } [a, b] = b - a + 1.$$

On en déduit immédiatement :

Corollaire 2.

Quel que soit l'entier naturel $n \neq 0$ tout ensemble fini de cardinal n est équipotent à $[1, n]$.

B. 12 CONCLUSION

En admettant un petit nombre de résultats :

- La relation dans la classe de tous les ensembles « il existe une injection de A dans B » est une relation d'ordre total (§ B.6),
- Il existe un ensemble, noté $\mathbb{N}$, dont les éléments sont tous les cardinaux finis (§ B.9),
- Toute partie non vide de $\mathbb{N}$ a un plus petit élément (§ B.9 théorème 10),

nous avons retrouvé tous les résultats *admis en bloc* aux paragraphes 1.3 et 1.4 (propriétés de $(\mathbb{N}, +, \times, \leqslant)$) et 1.6 a (premières propriétés des cardinaux finis). Le lecteur ayant étudié cette annexe B trouvera dans les autres paragraphes du chapitre 1 la suite naturelle des propriétés étudiées dans cette annexe B; notons en particulier cette propriété essentielle démontrée au § 1.6 c : *Toute partie non vide de* $\mathbb{N}$ *est finie si et seulement si elle est majorée.*

ANNEXE C

Groupe commutatif $(\mathbb{Z}, +)$

L'exposé ci-dessous donne les démonstrations des résultats admis en bloc au § 2.1 b.

C. 1 INTRODUCTION

L'ensemble $\mathbb{N}$ muni de l'addition, c'est-à-dire $(\mathbb{N}, +)$ possède les propriétés suivantes : l'addition est *associative*, *commutative*, possède un *élément neutre*, *zéro*, et *tout élément* de $\mathbb{N}$ est *régulier* pour l'addition.
Nous cherchons un groupe commutatif G tel que $\mathbb{N}$ soit une partie de G et que la loi interne dans G prolonge celle de $\mathbb{N}$; si nous notons également par le signe $+$ la loi dans G, ceci revient à dire que nous cherchons un groupe $(G, +)$ tel que $(\mathbb{N}, +)$ soit une partie stable de ce groupe.
Remarquons que si $(G, +)$ répond à la question et si $(G, +)$ est sous-groupe d'un groupe commutatif $(G', +)$, alors $(G', +)$ répond aussi à la question. Nous chercherons donc un groupe G qui soit le plus petit possible, pour la relation d'inclusion.
Récapitulons les propriétés de l'objet $(G, +)$ que nous cherchons :

1. $(G, +)$ est un groupe commutatif,
2. $(\mathbb{N}, +)$ est une partie stable de $(G, +)$,
3. Il n'existe pas de sous-groupe de G distinct de G tel que $\mathbb{N}$ soit partie stable de ce sous-groupe.

Le problème ainsi posé est appelé **problème de la symétrisation de l'addition dans** $\mathbb{N}$.
Appliquons la méthode générale utilisée lorsque l'on a à construire un objet — ici un groupe commutatif — satisfaisant à certaines propriétés : c'est-à-dire supposons qu'il existe un ensemble G, muni d'une addition, possédant les propriétés 1, 2 et 3 ci-dessus.
Soit deux entiers naturels quelconques a et a', ce sont des éléments de $\mathbb{N}$, donc de G. L'équation

$$x + a' = a$$

n'a de solution dans $\mathbb{N}$ que si $a' \leqslant a$. Dans G elle aura une solution $a - a'$ et ceci quels que soient les entiers naturels a et a'. Donc à tout couple (a, a') de $\mathbb{N} \times \mathbb{N}$ est associé un élément de G $x = a - a'$. Mais à cet élément x de G n'est pas associé un couple unique d'entiers naturels; en effet à tous les couples (b, b') de $\mathbb{N} \times \mathbb{N}$ tels que $b - b' = a - a'$ est associé le même élément x de G.
Pour construire G nous sommes donc amenés à considérer l'ensemble $\mathbb{N} \times \mathbb{N}$ muni de la relation qui, entre les couples (a, a') et (b, b'), s'écrit $b - b' = a - a'$. Lorsque nous commençons notre étude, nous ne connaissons que $(\mathbb{N}, +)$; nous ne pouvons donc pas considérer cette relation qui fait intervenir $-a'$ et $-b'$; mais la relation considérée est équivalente à $a + b' = b + a'$ où n'interviennent que des éléments de $\mathbb{N}$.
Enfin si a, a', b, b' sont des éléments quelconques de $\mathbb{N}$ et si x et y sont les éléments de G vérifiant

$$x + a' = a \quad \text{et} \quad y + b' = b,$$

on aura

$$x + y = (a - a') + (b - b') = (a + b) - (a' + b')$$

donc au couple $(a + b, a' + b')$ de $\mathbb{N} \times \mathbb{N}$ est associé l'élément $x + y$ de G; comme aux couples (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$ sont associés respectivement x et y, éléments de G, nous sommes amenés tout naturellement à définir une addition dans $\mathbb{N} \times \mathbb{N}$ en posant

$$(a, a') + (b, b') = (a + b, a' + b').$$

L'étude précédente nous conduit donc à considérer l'ensemble $\mathbb{N} \times \mathbb{N}$ muni

1° De la *relation* $\mathcal{R}$ définie, quels que soient (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$, par

$$(a, a') \mathcal{R} (b, b') \Longleftrightarrow (a + b' = b + a').$$

2° De l'*addition* définie, quels que soient (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$, par

$$(a, a') + (b, b') = (a + b, a' + b').$$

Remarquons que la relation $\mathcal{R}$ et l'addition définies dans $\mathbb{N} \times \mathbb{N}$ ne dépendent que des propriétés de $(\mathbb{N}, +)$. Nous allons donc commencer par étudier les propriétés de $\mathbb{N} \times \mathbb{N}$ muni de la relation $\mathcal{R}$ et de l'addition que nous venons de définir.

C. 2 ÉTUDE DE $\mathbb{N} \times \mathbb{N}$ MUNI DE LA RELATION $\mathcal{R}$ ET DE L'ADDITION DÉFINIES CI-DESSUS

a) Propriétés de la relation $\mathcal{R}$.

Quel que soit (a, a') de $\mathbb{N} \times \mathbb{N}$, on a

$$a + a' = a + a';$$

la relation $\mathcal{R}$ est donc *réflexive*.

Quels que soient (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$, on a (symétrie de l'égalité)

$$(a + b' = b + a') \Longrightarrow (b + a' = a + b');$$

la relation $\mathcal{R}$ est donc *symétrique*.

Quels que soient les couples (a, a'), (b, b'), (c, c'), la relation

$$(a, a') \mathcal{R} (b, b') \quad et \quad (b, b') \mathcal{R} (c, c'),$$

c'est-à-dire

$$a + b' = b + a' \quad et \quad b + c' = c + b',$$

implique

$$(a + b') + (b + c') = (b + a') + (c + b'),$$

ou, en utilisant l'associativité et la commutativité de l'addition dans $\mathbb{N}$,

$$(a + c') + (b + b') = (c + a') + (b + b'),$$

ou encore, en utilisant le fait que dans $\mathbb{N}$ tout élément est régulier,

$$a + c' = c + a',$$

c'est-à-dire

$$(a, a') \mathcal{R} (c, c');$$

la relation $\mathcal{R}$ est donc *transitive*.

Lemme 1.

La relation $\mathcal{R}$ est une relation d'équivalence.

Nous pouvons donc considérer l'ensemble-quotient $\dfrac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$; la classe, modulo $\mathcal{R}$, de représentant (a, a') se notera $\dot{(a, a')}$.

Quels que soient (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$ on a

$$[(a, a') \equiv (b, b') \pmod{\mathcal{R}}] \Longleftrightarrow [\dot{(a, a')} = \dot{(b, b')}] \Longleftrightarrow [a + b' = b + a'].$$

En particulier, on voit que, quel que soit x de $\mathbb{N}$, on a

$$\dot{(a, a')} = \dot{(a + x, a' + x)};$$

plus particulièrement encore, quel que soit x de $\mathbb{N}$, on a

$$\dot{(0, 0)} = \dot{(x, x)}.$$

b) Propriétés de l'addition définie sur $\mathbb{N} \times \mathbb{N}$.

La formule définissant la somme de deux couples quelconques (a, a') et (b, b') de $\mathbb{N} \times \mathbb{N}$

$$(a, a') + (b, b') = (a + b, a' + b')$$

montre immédiatement que cette addition définie dans $\mathbb{N} \times \mathbb{N}$ est *associative* et *commutative* (vérifiez le à titre d'exercice).
D'autre part, on a, quel que soit (a, a') de $\mathbb{N} \times \mathbb{N}$,

$$(0, 0) + (a, a') = (a, a') + (0, 0) = (a + 0, a' + 0) = (a, a'),$$

donc cette addition possède l'élément neutre $(0, 0)$.
Enfin tout élément est régulier; en effet, quels que soient (a, a'), (b, b'), (c, c') de $\mathbb{N} \times \mathbb{N}$, l'égalité

$$(a, a') + (c, c') = (b, b') + (c, c'),$$

c'est-à-dire $$(a + c, a' + c') = (b + c, b' + c')$$

implique (égalité des couples)

$$a + c = b + c \quad et \quad a' + c' = b' + c',$$

ou encore (régularité de tout élément pour l'addition dans $\mathbb{N}$)

$$a = b \quad et \quad a' = b'$$

c'est-à-dire $$(a, a') = (b, b').$$

Lemme 2.

L'addition définie dans $\mathbb{N} \times \mathbb{N}$ est associative, commutative, a $(0, 0)$ pour élément neutre et, pour elle, tout élément de $\mathbb{N} \times \mathbb{N}$ est régulier.

L'ensemble $\mathbb{N} \times \mathbb{N}$ étant muni d'une relation d'équivalence $\mathcal{R}$ et d'une addition, cherchons à définir à partir de l'addition dans $\mathbb{N} \times \mathbb{N}$ une loi interne dans $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$. Il est tout à fait naturel de penser à prendre pour composé de $\dot{(a, a')}$ et $\dot{(b, b')}$ la classe de la somme de leurs représentants respectifs c'est-à-dire

$$\dot{(a, a')} + \dot{(b, b')} = \dot{(a + b, a' + b')}.$$

Mais le composé des deux classes $\dot{(a, a')}$ et $\dot{(b, b')}$ ne doit pas changer si l'on remplace (a, a') et (b, b') par des couples (a_1, a_1'), (b_1, b_1') qui leur sont respectivement équivalents, modulo $\mathcal{R}$. Nous allons voir que cette propriété est bien vérifiée.

c) Compatibilité de l'addition et de la relation $\mathcal{R}$ définies dans $\mathbb{N} \times \mathbb{N}$.

Considérons deux éléments quelconques $\dot{(a, a')}$ et $\dot{(b, b')}$ de $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$; soient (a_1, a_1') et (b_1, b_1') des représentants respectifs quelconques de chacune de ces classes. Nous avons

$$(a, a') \equiv (a_1, a_1') \quad \text{et} \quad (b, b') \equiv (b_1, b_1') \pmod{\mathcal{R}},$$

c'est-à-dire $$a + a_1' = a_1 + a' \quad et \quad b + b_1' = b_1 + b';$$

d'où $$(a + a_1') + (b + b_1') = (a_1 + a') + (b_1 + b'),$$

ou encore en utilisant l'associativité et la commutativité de l'addition dans $\mathbb{N}$

$$(a + b) + (a_1' + b_1') = (a_1 + b_1) + (a' + b')$$

c'est-à-dire $$(a + b, a' + b') \equiv (a_1 + b_1, a_1' + b_1') \pmod{\mathcal{R}},$$

ou enfin $$(a, a') + (b, b') \equiv (a_1, a_1') + (b_1, b_1') \pmod{\mathcal{R}}.$$

Lemme 3.

Les sommes de deux représentants quelconques de deux classes, modulo $\mathcal{R}$, sont toutes équivalentes entre elles, modulo $\mathcal{R}$.

On exprime cette propriété en disant que dans $\mathbb{N} \times \mathbb{N}$ l'addition et la relation d'équivalence $\mathcal{R}$ **sont compatibles.**

C. 3 GROUPE $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$. RELATION AVEC $(\mathbb{N}, +)$. GROUPE $(\mathbb{Z}, +)$

a) Groupe $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$.

Prenons deux classes quelconques α et β, modulo $\mathcal{R}$; quels que soient le représentant (a, a') de α et (b, b') de β, tous les couples $(a + b, a' + b')$ appartiennent, d'après le lemme 3, a une même classe γ, modulo $\mathcal{R}$.

Par **définition** nous dirons que cette classe γ est le composé des classes α et β. La loi interne ainsi définie sur $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ est appelée **loi-quotient** *de l'addition dans* $\mathbb{N} \times \mathbb{N}$ *par la relation d'équivalence* $\mathcal{R}$, *compatible avec cette addition*; nous la noterons $\dot{+}$; on a donc, par définition, quels que soient les éléments $\dot{(a, a')}$ et $\dot{(b, b')}$ de $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$

$$\dot{(a, a')} \dot{+} \dot{(b, b')} = \dot{(a + b, a' + b')}.$$

L'addition, notée $\dot{+}$, des classes, modulo $\mathcal{R}$, se ramenant à l'addition, notée $+$, des couples, est, comme cette dernière, *associative* et *commutative*.

D'autre part, quelle que soit la classe $\dot{(a, a')}$ on a

$$\dot{(0, 0)} \dot{+} \dot{(a, a')} = \dot{(a, a')} \dot{+} \dot{(0, 0)} = \dot{(a + 0, a' + 0)} = \dot{(a, a')}.$$

Donc $\dot{(0, 0)}$ est *élément neutre* pour l'addition notée $\dot{+}$.

Enfin, quelle que soit la classe $\dot{(a, a')}$ nous avons

$$\dot{(a, a')} \dot{+} \dot{(a', a)} = \dot{(a + a', a' + a)} = \dot{(0, 0)}.$$

Donc toute classe est *symétrisable*. Concluons :

Lemme 4.

$\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$ est un groupe commutatif.

Une question se pose : quel rapport y a-t-il entre le groupe obtenu et le groupe G *que nous cherchions ou encore entre* $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$ *et* $(\mathbb{N}, +)$*?*

Quels que soient a et a' *de* $\mathbb{N}$, *le groupe* G *que nous cherchons doit comprendre toutes les solutions de* $x + a' = a$; *or certaines de ces solutions appartiennent à* $\mathbb{N}$ *elles correspondent aux couples* (a, a') *tels que* $a' \leqslant a$ *c'est-à-dire tels que* $a - a' \in \mathbb{N}$; *pour de tels couples on a*

$$\dot{(a, a')} = \dot{(a - a', 0)}$$

d'après une remarque faite à la fin du § C.2 a.

Nous allons donc étudier la partie $\mathbb{N}'$ *de* $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ *définie par*

$$\mathbb{N}' = \left\{ \dot{(a, a')} \in \frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}} \;\middle|\; a' \leqslant a \right\}.$$

b) Relation entre $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$ et $(\mathbb{N}, +)$.

D'après une remarque faite ci-dessus $\mathbb{N}'$ est l'ensemble de toutes les classes de la forme $\dot{(x, 0)}$ où x est un *entier naturel quelconque*. Quels que soient les entiers naturels x et y, on a

$$\dot{(x, 0)} \dot{+} \dot{(y, 0)} = \dot{(\widetilde{x + y}, 0)}.$$

Donc $\mathbb{N}'$ est une *partie stable de* $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$.

Considérons l'application φ

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}'$$
$$x \longmapsto \dot{(x, 0)}.$$

L'ensemble $\mathbb{N}'$ étant l'ensemble de toutes les classes de la forme $\dot{(x, 0)}$, où x est un entier naturel quelconque, l'application φ est *surjective*.
D'autre part, quels que soient x et y de $\mathbb{N}$, on a

$$(\dot{(x, 0)} = \dot{(y, 0)}) \Longrightarrow (x + 0 = 0 + y) \Longrightarrow (x = y);$$

donc l'application φ est *injective*.
Par conséquent φ est une bijection.
Enfin, quels que soient x et y de $\mathbb{N}$, on a

$$\varphi(x + y) = \dot{(\widetilde{x + y}, 0)} = \dot{(x, 0)} \dot{+} \dot{(y, 0)}$$

c'est-à-dire

$$\varphi(x + y) = \varphi(x) \dot{+} \varphi(y).$$

Donc φ définit un *isomorphisme* de $(\mathbb{N}, +)$ sur $(\mathbb{N}', \dot{+})$. Concluons :

Lemme 5.

La partie $\mathbb{N}'$ de $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ décrite par toutes les classes de la forme $\dot{(x, 0)}$ est une partie stable de $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$ et $(\mathbb{N}', \dot{+})$ est isomorphe à $(\mathbb{N}, +)$.

c) Groupe $(\mathbb{Z}, +)$.

Le groupe $\left(\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}, \dot{+}\right)$ ne contient pas $\mathbb{N}$, mais seulement une *partie stable* $\mathbb{N}'$ telle que $(\mathbb{N}', \dot{+})$ soit *isomorphe* à $(\mathbb{N}, +)$.
Or nous savons que si $(E, \top)$ et $(E', \top')$ sont isomorphes les propriétés de la loi interne $\top$ sur E et de la loi interne $\top'$ sur E' sont *exactement les mêmes* : il n'y a donc aucun inconvénient à **identifier** les éléments $\dot{(x, 0)}$ de $\mathbb{N}'$ et x de $\mathbb{N}$ associés par l'isomorphisme φ. Nous poserons donc, quel que soit x de $\mathbb{N}$

$$\dot{(x, 0)} = x.$$

En particulier $\dot{(0, 0)} = 0$ et $\dot{(1, 0)} = 1$.

Définition.

L'ensemble obtenu en identifiant dans $\frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$ chaque élément de la forme $\dot{(x, 0)}$ avec l'entier naturel x est appelé ensemble des **entiers relatifs.**
On le note $\mathbb{Z}$.

Nous noterons aussi $+$ l'addition dans $\mathbb{Z}$. L'opposé de $\dot{(a, a')}$ se notera $-\dot{(a, a')}$; nous avons vu que l'on a

$$-\dot{(a, a')} = \dot{(a', a)};$$

en particulier pour tout entier naturel x on a

$$-\dot{(x, 0)} = \dot{(0, x)}.$$

Nous avons, dans ces conditions, obtenu les résultats suivants :

1. $(\mathbb{Z}, +)$ est un groupe commutatif.
2. $(\mathbb{N}, +)$ est une partie stable de $(\mathbb{Z}, +)$.

Enfin, quel que soit $\dot{(a, a')}$ de $\mathbb{Z}$, on a

si $a' \leqslant a$ $\qquad \dot{(a, a')} = \dot{(a - a', 0)} = a - a' \in \mathbb{N}$

si $a \leqslant a'$ $\qquad \dot{(a, a')} = \dot{(0, a' - a)} = -\dot{(a' - a, 0)} \in (-\mathbb{N})$

en notant par le symbole $-\mathbb{N}$, la partie de $\mathbb{Z}$, ensemble des opposés des éléments de $\mathbb{N}$. On voit donc que l'on a

$$\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) \quad \text{et} \quad \mathbb{N} \cap (-\mathbb{N}) = \{0\}.$$

Tout groupe commutatif $(G, +)$ contenant la partie stable $\mathbb{N}$ doit contenir $-\mathbb{N}$ donc $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$ par conséquent il n'y a pas de sous-groupe de $\mathbb{Z}$ distinct du groupe $(\mathbb{Z}, +)$ qui admette $\mathbb{N}$ pour partie stable. Donc le groupe $(\mathbb{Z}, +)$ est un groupe répondant aux conditions du problème posé au § C.1.

Théorème de symétrisation de l'addition de $\mathbb{N}$.

Il existe un ensemble $\mathbb{Z}$, muni d'une addition, tel que

1. $(\mathbb{Z}, +)$ est un groupe commutatif.
2. $(\mathbb{N}, +)$ est une partie stable de $(\mathbb{Z}, +)$.
3. Il n'existe pas de sous-groupe de $\mathbb{Z}$, distinct de $\mathbb{Z}$, tel que $\mathbb{N}$ soit une partie stable de ce sous-groupe.

REMARQUES

1. On peut se demander si le groupe $(\mathbb{Z}, +)$ est le seul groupe vérifiant les conditions posées au § C.1. Nous allons voir que la réponse diffère suivant le sens attribué au mot « unique ».

Soit $(G, \top)$ un groupe commutatif isomorphe au groupe $(\mathbb{Z}, +)$; c'est-à-dire il existe une bijection f de $\mathbb{Z}$ sur G telle que, pour tout x et tout y de $\mathbb{Z}$, on ait

$$f(x + y) = f(x) \top f(y).$$

D'après l'isomorphisme f, $\mathbb{N}$ étant une partie stable de $\mathbb{Z}$, $f(\mathbb{N})$ est une partie stable de $(G, \top)$.

D'autre part il est évident que la restriction φ_1, de f à $\mathbb{N}$ et prenant ses valeurs dans $f(\mathbb{N})$, est un isomorphisme de $(\mathbb{N}, +)$ sur $(f(\mathbb{N}), \top)$; en identifiant $\mathbb{N}$ et $f(\mathbb{N})$, de même que nous avons identifié $\mathbb{N}$ et $\mathbb{N}'$ partie stable de $\dfrac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$, nous voyons que G satisfait aux deux premières conditions du problème de symétrisation; ce groupe G satisfait aussi à la troisième condition, car, s'il existait, pour G, un sous-groupe propre satisfaisant aux deux premières conditions, l'isomorphisme f montre que la même propriété serait vérifiée pour le groupe $\mathbb{Z}$, ce qui est faux.

Donc tout groupe $(G, \top)$ *isomorphe à* $(\mathbb{Z}, +)$ *est solution du problème de symétrisation de l'addition dans* $\mathbb{N}$.

Nous admettrons que les *seules solutions* de ce problème de symétrisation sont les *groupes isomorphes au groupe* $\mathbb{Z}$.

Donc, au sens strict, un ensemble G vérifiant les trois conditions du § C.1 n'est pas unique.

Mais, les mathématiciens s'intéressant davantage aux relations entre objets qu'aux objets eux-mêmes et tous les groupes commutatifs étant isomorphes entre eux, on convient de dire que le problème de la symétrisation de l'addition dans $\mathbb{N}$, par un groupe commutatif, a une **solution unique à un isomorphisme près.**

2. Les considérations des § C.2 et C.3 n'utilisent, parmi toutes les propriétés des entiers naturels, que les faits suivants :

1. l'addition dans $\mathbb{N}$ est associative,
2. — — — commutative,
3. — — possède un élément neutre,
4. tout élément de $\mathbb{N}$ est régulier pour l'addition dans $\mathbb{N}$.

Nous pourrions donc recommencer toute la théorie à partir de (E, $\top$) possédant les 4 propriétés rappelées ci-dessus.

EXERCICES

1. **Résoudre le problème de la symétrisation de la multiplication dans $\mathbb{N}^*$. Le groupe obtenu est $(\mathbb{Q}_+^*, \times)$.**
2. **Montrer que la propriété 3, la loi $\top$ possède un élément neutre, est superflue pour résoudre le problème de la symétrisation de la loi $\top$ dans E. (Les notations sont plus compliquées, l'élément neutre de $\frac{E \times E}{\mathcal{R}}$ est $\widehat{(x, x)}$, quel que soit x de E et la partie E′ de $\frac{E \times E}{\mathcal{R}}$ isomorphe à (E, $\top$) est décrite par les éléments de la forme $\widehat{(x \top y, y)}$, x et y étant des éléments quelconques de E). Par exemple, 2 $\mathbb{N}^*$ représentant l'ensemble des entiers naturels pairs *non nuls*, résoudre le problème de la symétrisation de la multiplication dans 2 $\mathbb{N}^*$.**

INDEX

Addition des applications linéaires : 208
— des matrices 211
affixe (d'un point, d'un vecteur) 223
algèbre de Boole 267
— sur $\mathbb{R}$ 248
algorithme d'Euclide 81
anneau 52
— commutatif 53
— intègre 55
— totalement ordonné 56
— unitaire 53
application additive 269
— canonique de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ 69
— croissante 269
— fortement additive 269
— linéaire 208
— mesurable 271
angle 234
Archimède (lemme) 32
argument (d'un nombre complexe) .. 236
Base d'un espace vectoriel 204
— canonique de $\mathbb{R}^n$ 205
— orthonormée 222
Bezout (égalité de) 79
binôme (formule du) 135
borné 15
borne supérieure (resp. inférieure) .. 16
— (axiome de la) 136
Caractéristique d'un décimal 174
cardinal d'un ensemble fini 22
carré scalaire 222
coefficient dans une combinaison linéaire 203
— de corrélation 288
— d'une fonction linéaire ... 116
coefficients binomiaux 31
combinaison linéaire 203
compatibilité entre une relation d'é-quivalence et une loi interne. 66
congruence modulo n 63
coordonnées d'un vecteur 205
corps commutatif 75
— des nombres complexes 215
cosinus 235
Demi-droite vectorielle 234
densité de $\mathbb{Q}$ dans $\mathbb{R}$ 148
développement décimal illimité d'un réel 176
développement décimal illimité périodique d'un réel 180
développement décimal illimité propre (resp. impropre) 180
dimension d'un espace vectoriel 205
distance 127
— euclidienne 223
diviseur de zéro 55
division euclidienne dans $\mathbb{N}$ 32
— $\mathbb{Z}$ 58
droite vectorielle 205
Ecart type 285
écriture normalisée d'un décimal 183
élément régulier 14
encadrement 181
ensemble (fini-infini) 21
entier naturel 17
— premier 90
— rationnel 48
— relatif 48
entiers étrangers 78
— dans leur ensemble. 85
entiers modulo n 64
— premiers entre eux 78
— premiers entre eux (dans leur ensemble) 85
équipotent 21
Eratosthène (crible d') 91
erreur 181
— relative 184
espace de probabilité 269
— probabilisable 268
— vectoriel sur $\mathbb{R}$ 201
espérance mathématique 283
Euclide (algorithme d') 81
exposant 128
Factorielle n 27
fonction linéaire 116
— de répartition 275

forme algébrique d'un nombre complexe 218
— trigonométrique d'un nombre complexe 237
Gauss (théorème de) 80
Groupe 47
Groupe commutatif totalement ordonné 51
Homomorphisme 70
— d'espace vectoriel. 207
i (nombre complexe *i*) 217
idéal 62
image d'une application linéaire 208
— d'un nombre complexe 223
incertitude 181
— relative 184
indice d'un terme d'une suite 149
intervalles de $\mathbb{N}$ 18
— de $\mathbb{R}$ 118
isométrie vectorielle 233
isomorphisme 73
— d'espace vectoriel ... 208
j (nombre complexe *j*) 243
Limite d'une suite réelle 154
— infinie 156
linéarisation 247
loi conjointe 277
— de probabilité 275
— induite 48
— marginale 277
— quotient 66
Majorant 15
mantisse d'un décimal 174
matrice d'une application linéaire .. 210
— scalaire 215
minorant 15
module d'un nombre complexe 225
Moivre (formule de) 242
multiple d'un entier relatif 59
multiplication externe 201
Nombre complexe 215
— imaginaire pur 219
nombres complexes conjugués 219
nombre décimal 169
— irrationnel 136
— rationnel 123
— réel 112
— — négatif (resp. positif)... 119
norme euclidienne 222
noyau d'une application linéaire 208
Ordonné 14
ordre naturel sur $\mathbb{N}$ 17
orientation de $\mathcal{E}_2$ 235
Partie entière d'un réel 147
— génératrice d'un espace vectoriel 204
— imaginaire d'un nombre complexe 218
— irrégulière d'un développement décimal périodique 180
— libre d'un espace vectoriel .. 204
partie majorée d'un ensemble ordonné 15
— minorée d'un ensemble ordonné 15
— réelle d'un nombre complexe . 218
parties adjacentes de $\mathbb{R}$ 142
partie stable d'un espace vectoriel pour la multiplication externe 203
partie stable pour une loi interne 48
période d'un développement décimal périodique 180
p.g.c.d. de deux entiers relatifs 78
— de plusieurs entiers relatifs . 84
plan affine 222
— euclidien 222
— vectoriel 205
— — euclidien 222
— — — orienté . 235
plus grand élément d'une partie d'un ensemble ordonné 16
plus petit d'un ensemble ordonné ... 16
point image d'un nombre complexe . 223
p.p.c.m. de deux entiers relatifs 87
— de plusieurs entiers relatifs.. 89
probabilité 269
probabilité image 274
produit scalaire 221
progression arithmétique 152
— géométrique 153
prolongement d'une loi interne 48
puissance entière d'un réel 128
Quotient dans la division euclidienne dans $\mathbb{N}$ 33
Racine $n^{\text{ième}}$ positive d'un réel positif 145

racines carrées d'un nombre complexe 229
— $n^{\text{ième}}$ d'un nombre complexe 242
récurrence 20
repère d'un plan affine 222
— orthonormé 223
reste dans la division euclidienne dans $\mathbb{N}$ 33
rotation vectorielle 234
Scalaire (dans un espace vectoriel) .. 202
segments emboîtés (dans $\mathbb{R}$) 142
série géométrique 167
sinus 235
somme d'idéaux 77-84
sous-anneau 61
sous-corps 110
sous-groupe 58
sous-espace vectoriel 203
— engendré par $\{a_1, \ldots, a_n\}$ ... 204
— propre 203
suite arithmétique 151
— d'éléments d'un ensemble 24
— de nombres réels 149
— extraite 25-150
suite finie 25
— géométrique 153
— infinie 25
— réelle 149
— — convergente 154
— stationnaire 25-150
système de rémunération 33
Taux d'erreur (resp. d'incertitude) .. 184
terme d'indice n 149
tribu 267
Valeur absolue 52-125
— approchée par défaut (ou par excès) 181
— approchée par défaut à α^{-n} près 147
— approchée par défaut à 10^{-k} près 172
valeurs approchées usuelles 186
variable aléatoire 271
variables aléatoires indépendantes ... 280
variance 285
vecteur (dans un espace vectoriel) .. 202
— image d'un nombre complexe 223
vecteurs linéairement dépendants .. 204
— indépendants . 204

Table des matières

Avant-Propos 3

Programme de Terminale C 5
Programme de Terminale E 9

1 |
Entiers naturels 13

2 |
Entiers relatifs 47

3 |
Nombres réels 109

4 |
Nombres complexes 201

5 |
Probabilités 265

Annexe A

Lois de composition interne 299

Annexe B

Introduction à l'étude des cardinaux et des entiers naturels 304

Annexe C

Groupe commutatif $(\mathbb{Z}, +)$ 324

Index 331

Imprimé en France par FIRMIN-DIDOT S.A.
Dépôt légal : 3e trimestre 1975
N° d'édition : C 19950 VII (AU.c.VII) — N° d'impression : 7747

183 147